We encourage you to e-mail your comments to us at: strategicstudiesquarterly@maxwell.af.mil.

SSQ

STRATEGIC STUDIES QUARTERLY

SUMMER 2011 VOL. 5, NO. 2

We encourage you to e-mail your comments to us at: strategicstudiesquarterly@maxwell.af.mil.

SSQ

Strategic Studies Quarterly (*SSQ*) (ISSN 1936-1815) is published quarterly by Air University Press, Maxwell AFB, AL.

We encourage you to e-mail your comments to us at: strategicstudiesquarterly@maxwell.af.mil.

Strategic Studies Quarterly

An Air Force–Sponsored Strategic Forum on National and International Security

VOLUME 5 SUMMER 2011 NUMBER 2

Commentary

Feature Article

Perspectives

Selected Online Book Reviews

Known and Unknown: A Memoir
Donald Rumsfeld

Byting Back: Regaining Information Superiority
Martin Libicki, David C. Gompert, David Frelinger, and Raymond Smith

Occupying Iraq: A History of the Coalition Provisional Authority
James Dobbins, Seth G. Jones, Benjamin Runkle, and Siddharth Mohandas

Strategic US Foreign Assistance: The Battle between Human Rights and National Security
Rhonda L. Callaway and Elizabeth G. Matthews

The Military Transition: Democratic Reform of the Armed Forces
Narcis Serra

http://afri.au.af.mil/reviews.asp

Building a New Command in Cyberspace

Cybersecurity is vital to our nation. Part of our task at US Cyber Command is ensuring that our nation understands what it is that the White House, Congress, and the Department of Defense have charged us to do and why it is so important that it be done well. Constructing a new command while conducting operations is quite a challenge, especially in a time of rapid technological and policy changes, but this new command has produced results that have made our nation stronger and more secure and has already returned cybersecurity dividends on the investments of time and resources dedicated to its creation.

The Road to Full Operational Capability

US Cyber Command achieved full operational capability (FOC) on 31 October 2010 as a subunified command under US Strategic Command (USSTRATCOM). The road to FOC culminated roughly according to the timetable prescribed by the secretary of defense when he directed the establishment of the command back in June 2009. Initial operational capability (IOC) was originally projected to have been reached that October, but that date slipped to May 2010, when my nomination to serve as its first commander was confirmed by the Senate. We put the months between October 2009 and May 2010 to good use, however, building a consolidated staff to merge the two legacy organizations, Joint Functional Component Command for Network Warfare (JFCC-NW) and Joint Task Force for Global Network Operations (JTF-GNO), which together became Cyber Command. We also outlined the tasks needed to move us to FOC once the clock started running. Though the interval between initial capability in May and attaining full operational capability in October was only five months instead of the planned 12, we were able to attain several goals. Moreover, we did so while accelerating the tempo of daily operations that had been established by JTF-GNO and JFCC-NW.

Editor's Note: In March 2011 GEN Keith B. Alexander, USA, testified before the House Armed Services Committee's Subcommittee on Emerging Threats and Capabilities on the progress made in establishing US Cyber Command. This commentary reflects his statement on that occasion.

Despite the compressed schedule, the consolidated staff at Cyber Command accomplished a great deal by October 2010. We established a joint operations center, transferred operational control of the JTF-GNO mission set to Fort Meade, Maryland, and stood down JTF-GNO's 24/7 watch center in Arlington, Virginia; these steps helped USSTRATCOM disestablish JFCC-NW and JTF-GNO. The latter task took a considerable amount of planning and careful orchestration because JTF-GNO's activities and workforce had to be transitioned from Northern Virginia to Fort Meade, while ensuring that the daily functioning of the DoD information networks continued unimpaired. We established effective operational command and control processes for the consolidated mission sets. A joint intelligence operations center was established. Our service cyber components were formally assigned to USSTRATCOM, and we continued building relationships with key partners. We embedded liaison officers at the combatant commands and set conditions to expand their presence in larger cyber support elements. We deployed expeditionary teams to support operations in Iraq and Afghanistan. We also made progress in our support of operational planning by the combatant commanders and in building processes for them to issue requirements for cyber support. The command accomplished all of this without negative mission impact, keeping the department's operations secure while making the transition transparent to users of its information systems.

The command's fiscal year 2012 budget is projected to be $159 million, and our workforce at that point is slated to be 464 military personnel and 467 civilians, for a total of 931 employees. This team's overall mission is to plan, coordinate, integrate, synchronize, and conduct activities to direct the operations in defense of specified DoD information networks and be prepared, when directed, to conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure US and allied freedom of action in cyberspace, and deny the same to our adversaries. Last but not least, US Cyber Command continues to build synergy with the National Security Agency (NSA) to take advantage of the NSA's infrastructure and expertise, which remain crucial to our progress. Our collocation with the NSA allows the government to maximize our collective talent and capabilities.

Current Perspectives

Our leaders from President Obama on down have spoken of the importance to our nation of preserving our security in cyberspace and maintaining

our freedom of action in this new, unique, man-made domain. We face many challenges in doing so, especially in light of recent developments.

The cyber threat continues to evolve, posing dangers that far exceed the 2008 breach of our classified systems that Deputy Secretary of Defense William Lynn described in his Fall 2010 *Foreign Affairs* article as a turning point for cybersecurity. Our nation now depends on access to cyberspace and the data and capabilities residing there; we are collectively vulnerable to an array of threats ranging from network instability, to criminal and terrorist activities, to state-sponsored capabilities that are progressing from exploitation to disruption to destruction. While we have not suffered disastrous or irreparable harm in cyberspace from any of these risk categories, we must be prepared to counter these threats.

Both external actors and insider threats pose significant challenges to our cybersecurity. No state actor, of course, has admitted to launching disruptive cyber attacks on another state. Yet incidents have occurred that look a great deal like such attacks. The cyber assaults on Estonia in 2007 spurred the United States and our NATO allies to deliberate regarding what in cyberspace would constitute an "armed attack" on an alliance member that would trigger the North Atlantic Treaty's provisions on collective defense. The following year, the invasion of Georgia coincided with precisely targeted cyber attacks, marking one of the first times we have seen such "cyber supporting fires." The coincidence was so perfect that independent observers concluded there was no coincidence—that the hackers who temporarily crippled the Georgian government's response and communications with the outside world had practiced their assaults and responded to official cues when they mounted them for real.

We have recently seen Internet access manipulated or curtailed by governments to suppress and disrupt even peaceful protests by their own citizens. In addition, we believe that state actors have developed cyber weapons to cripple infrastructure targets in ways tantamount to kinetic assaults; some of these weapons could potentially destroy hardware as well as data and software. The possibilities for destructive cyber effects, having long been mostly theoretical, have now been produced outside of the lab and are proliferating into national arsenals and possibly beyond, moving them a step closer to intentional use or accidental release. Segments of our nation's critical infrastructure are not prepared to handle this kind of threat.

We also watch with concern the growing capabilities of nonstate actors. The threats we see here are asymmetric, meaning that comparatively new

or lesser players can cause effects commensurate with state-sponsored actions. Although individuals with computer skills have independently shown that such attacks can be launched by even a lone actor with a laptop and a motive, we are chiefly focused on terrorists and well-organized cyber criminals. The former continue to grow more proficient in using the Internet as a medium for recruitment, coordination, and other activities, and they are becoming ever more sophisticated in doing so. Cyber criminals are more interested in the theft and exploitation of sensitive data that can bring them a profit, either directly through fraud or identity theft, or indirectly through the pirating of intellectual capital. Indeed, observers such as Senator Sheldon Whitehouse and a bipartisan team of colleagues last summer called this "the biggest transfer of wealth through theft and piracy in the history of mankind"—a transfer that has significantly lowered the cost for potential adversaries to close and counter our technological lead. Such activity is crime, of course, and belongs more properly in law enforcement than military channels, but when a prime target of such crime is our defense industrial base, we in the Department of Defense have a role to play in the response. We also find that state actors and terrorists can exploit the breaches and tools made by criminals, much as a dangerous pathogen opportunistically employs a disease vector to enter a host. Indeed, sometimes state and nonstate actors collaborate on matters of mutual interest.

Significant security challenges also emanate from poor cyber hygiene, inadvertent misuse, and malicious actions. After all, even the most astute malicious cyber actors—those who can break into almost any network that they really try to penetrate—are usually searching for targets of opportunity. They seek easy vulnerabilities in our system's security and then exploit them. Our own neglect thus makes us vulnerable. Unapplied software patches, firewalls left unattended, and antivirus suites that never get updated even in the US military cause us serious trouble, especially when a risk to one is a risk shared by all. Now multiply those problems across the government and the private sector, and realize that we have networked our vulnerabilities while segmenting our defenses among the .mil, .gov, .com, and .edu Internet domains. Each domain (and often each system) has been left to fend for itself against cyber actors who care little for legal distinctions and organizational boundaries. And finally there is the insider threat; some of the largest security breaches in history have originated from the inside.

The recent creation of Cyber Command has garnered a great deal of interest from foreign militaries and the governments that oversee them. We see frequent media reports on nations contemplating the creation of their own "cyber commands." This appears to be a sign not necessarily of a "militarization" of cyberspace but rather a reflection of the level of the concern with which civilian and military leaders around the world are viewing current problems. Many such steps are essentially defensive, and if so many nations are interested in improving their defenses, they might be more willing to talk about ways they can reduce common threats. There is a rough, de facto deterrence at the strategic level of cyberspace. Although no one knows how a cyber war would play out, even the most capable state actors seem to recognize that it is in no one's interest to find out the hard way. This concern has led to a certain degree of restraint by states that we deem capable of causing very serious cyber effects. Lest optimism obscure real threats, however, we must note that we have no certain capability to restrain the behavior of radical, non-state extremists.

In sum, our adversaries in cyberspace are highly capable. Our economy and society have become directly or indirectly dependent on access to and freedom of movement in cyberspace—and indeed our military is equally dependent on such access—and thus we cannot be content with a situation in which we are sometimes our own worst enemy.

Working toward the Future

US Cyber Command's efforts and planning aim to ensure that the DoD has done all it can to defend and deter determined adversaries, mitigate dangerous threats, and address nagging vulnerabilities, so that even our most capable opponents will know that interfering with our nation's equities in cyberspace is a losing proposition.

Our command faces serious challenges as it comes together to do urgently needed work in cyberspace. Its establishment reflects the department's need to manage cyber risk, secure freedom of action, and ensure the development of integrated capabilities. Our intent is to overcome the challenges we face through the concerted efforts of implementing the department's recently approved strategy for cyberspace. We will pursue resolution of the capacity, resources, and information technology efficiencies issues we face through the five strategic initiatives of that strategy. We intend to:

- treat cyberspace as a domain for the purposes of organizing, training, and equipping, so the DoD can take full advantage of its potential in military, intelligence, and business operations;
- employ new defense operating concepts, including active cyber defenses such as screening traffic, to protect DoD networks and systems;
- partner closely with other US government departments and agencies and the private sector to enable a whole-of-government strategy and an integrated national approach to cybersecurity;
- build robust relationships with US allies and international partners to enable information sharing and strengthen collective cybersecurity; and
- leverage the nation's ingenuity by recruiting and retaining an exceptional cyber workforce and enable rapid technological innovation.

Our first duty is to ensure that DoD networks are secure. Doing so is crucial to protecting our data, to maintaining our war-fighting potential, and ultimately to defending our nation. Until recently we all viewed our networks as a great force multiplier—the magic that let us put ordnance on target and dispatch planes, troops, and ships to where they were needed, when they had to be there. Today, however, we understand that those networks represent a serious vulnerability, and we dread the thought of someone getting inside to bring them down or, perhaps even worse, to make a few subtle changes to the integrity of our data that will bring all our military operations to a halt. Without fast, assured, and safe data flows, we will not be able to fight our adversaries in the way we as Americans think they should be fought. We are not necessarily close to losing that edge, but potential adversaries understand where it lies, and are certainly contemplating ways of blunting it in any future conflict.

US Cyber Command is working to preserve that information advantage in many ways. We are directing the operations of the department's information networks, which knit together seven million computing devices spread across fifteen thousand networks. The recent move of the Defense Information Systems Agency (DISA) to a new facility on Fort Meade has enabled even greater collaboration between our two organizations. Cyber Command and the DISA collaborate on a daily basis to monitor the functioning of DoD information networks. That work includes the maintenance of sensors to detect and block adversary activity in those networks, the inspection of security settings and practices, and

the investigation of real and suspected incidents. Together we are making progress in all of these areas, growing our ability to stop intrusions and adapt to changing adversarial practices almost as fast as they evolve. The new sensor capabilities we are deploying and the aggressive inspection regime now coming together will improve our situation even more.

We also plan—in partnership with the NSA—the defense of specified DoD information systems, knowing that we have to stay ahead of the cyber threat in technological terms. Here US Cyber Command and our partners in the department are working on ways of shifting to a different and more defensible architecture for providing information services to users. A year from now we should be well on our way to having a hardened architecture proven, deployed, and providing a new level of cybersecurity. The idea is to reduce vulnerabilities inherent in the current architecture and to exploit the advantages of "cloud" computing and thin-client networks, moving the programs and the data that users need away from the thousands of desktops we now use—each of which has to be individually secured—up to a centralized configuration that will give us wider availability of applications and data combined with tighter control over accesses and vulnerabilities and more timely mitigation of the latter. Moving to a cloud architecture has the advantages of producing economies of scale and reducing the department's information technology costs. This architecture also would seem at first glance to be vulnerable to insider threats—indeed, no system that human beings use can be made immune to abuse—but we are convinced the controls and tools that will be built into the cloud will ensure that people cannot see any data beyond what they need for their jobs and will be swiftly identified if they make unauthorized attempts to access data.

Over the next year we hope to "operationalize" our department's networks. We will, of course, continue to do this with full regard for and protection of the privacy and civil liberties of all Americans as well as in compliance with all applicable laws and regulations. The idea is to transform DoD information systems from something to be passively guarded into a suite of capabilities that offer our commanders and senior leaders opportunities to adjust our defenses. If people who seek to harm us in cyberspace learn that doing so is costly and difficult, we believe we will see their patterns of behavior change. The technology is ready.

Our command's mission document states that we coordinate, integrate, and synchronize activities to direct the operations and defense of DoD

networks. In practice, that means we spend a great deal of time talking with leaders and experts in the department, the US government, private industry, and other nations as well. This effort begins, of course, with US Cyber Command's service cyber components, which provide the forces that implement our plans and execute our directives—Army Cyber Command, Marine Corps Forces Cyber Command, Fleet Cyber Command, and Air Force Cyber Command. We are still maturing the ways in which we and they will interact to support and be supported by the geographic combatant commands in various situations. Our mission depends as well on the work of the NSA, which provides the expertise and intelligence that are indispensable to understanding what is happening in cyberspace. We are constantly engaged with the DISA as well, and our relationship with it will likely change substantially and become even closer in the near future.

We have also strengthened our strategic partnership with the Department of Homeland Security (DHS) in accord with the recent agreement concluded by Secretaries Robert Gates and Janet Napolitano. A senior DHS official now works at the NSA with us, leads a DHS–DoD joint coordination element that was also established by the agreement, and attends many of our leadership meetings. Several government agencies are also represented 24 hours a day in our joint operations center. These measures, along with complementary measures at the DHS and other partners, should provide a whole-of-government awareness of what everyone is seeing so that we can plan for and execute authorized and coordinated joint actions in the event of an emergency. Finally, we are active players in the Defense Department's productive discussions between government and industry over how to share information regarding common threats and potential ways of mitigating them. The vast majority of our military's information rides on commercial infrastructure, and thus we need to develop shared insights into those dependencies for mission assurance purposes.

The second part of our mission at Cyber Command is to be prepared to conduct full-spectrum military cyberspace operations to enable actions in all domains. As I noted above, state and nonstate actors have already experimented with ways to harass or attack rival governments, whether to make a strategic point or in conjunction with kinetic attacks. Our military and our nation would be unwise to assume that we have seen the last of such attacks. We are prepared, when directed and in full compliance with applicable laws, to respond when we or our allies are threatened or subjected

to the use of force in the cyberspace. The president has emphasized that our digital infrastructure is a strategic national asset and has insisted that preparing our government for the task of protecting strategic national assets in cyberspace is a national security priority. Our efforts to do this are designed to achieve two goals:

- First, we protect US and allied freedom of action in cyberspace. It is no longer possible to conceive of our nation functioning properly or even defending itself without the ability to create, transmit, and secure masses of digitized data. Making our access to cyberspace impossible or even problematic would represent a strategic threat to America's vital interests—one that our command has been established and tasked to prevent with respect to DoD operations in cyberspace. Furthermore, our cybersecurity is inextricably linked with that of our allies, and our interests in cyberspace can also coincide with those of other states with whom we have less-formal ties. The lack of geographic borders in cyberspace means that a threat to one can be a threat to all, which gives us a real incentive to share situational awareness and best practices that help to protect our military, government, and private networks and data.

- Second, when directed, we need to deny freedom of action in cyberspace for our adversaries. As with all activities the DoD pursues, operations are only executed with a clear mission and under clear authorities, and they are governed by all applicable laws, including the law of armed conflict. We cannot afford to allow cyberspace to be a sanctuary where real and potential adversaries can marshal forces and capabilities to use against us and our allies. This is not a hypothetical danger; in conflict areas where US forces are engaged we have indeed seen the Internet used for recruiting, fundraising, operational training, and other activities directed against our service personnel and coalition partners. At Cyber Command much of our focus is on helping our troops in the field limit their vulnerabilities in and from cyberspace. This effort reflects the likelihood that, henceforth, all conflicts will have some cyber aspect, and our efforts to understand this development will be crucial to the future security of the United States.

Conclusion

The Department of Defense took an important step for our nation in creating US Cyber Command and declaring it to be fully operational capable. At Cyber Command we have a mission to actively manage the department's information networks—not just to defend them but also to use them as a tool to assist our warfighters, planners, and commanders by preserving their freedom of action—and also to be as ready to use our own capabilities to disrupt any adversarial use of cyberspace against US interests. The command is seeking to:

- increase the capacity of the cyber workforce;
- implement and exploit, in a strengthened partnership with NSA, the transformation of the department's networks;
- work with the combatant commands to synchronize processes and planning to deliver the joint effects they require;
- extend cyber defense capabilities across US government networks through supporting partnerships with the NSA and the DHS as it works to secure federal, civilian, non-national security systems; and,
- with the DHS, increase government dialogue with private partners on the protection of our nation's critical infrastructure.

US Cyber Command operates with respect for civil liberties and in compliance with the laws governing the privacy of our fellow Americans, in accord with the directives of the national command authority, and in conjunction with mission partners in the Departments of Defense and Homeland Security, law enforcement, the intelligence community, industry, and academia. We do not see the security of our nation and the protection of civil liberties and privacy as a "balance"; rather, we believe we can and must defend both. I am confident that together we will succeed.

GEN Keith B. Alexander, USA
Commander, US Cyber Command
Director, National Security Agency
Chief, Central Security Service

Maintaining Flexible and Resilient Capabilities for Nuclear Deterrence

Keith B. Payne

Is NUCLEAR DETERRENCE an important element in US and allied security? If so, how many and what types of nuclear weapons are adequate for this purpose? These questions get to the heart of contemporary and decades-old nuclear policy debates, because most US nuclear policy initiatives are justified or criticized according to judgments regarding their potential effects on the US capacity to deter opponents. Most recently, the capability of our forces to help assure allies via extended deterrence, including the "nuclear umbrella," has been emphasized as a metric for US forces.[1] Using deterrence, extended deterrence, and assurance as a basis for judging the adequacy of US nuclear forces is appropriate because they are primary national security goals.

Attempts to render judgments about the adequacy of US nuclear forces usually proceed as if confident, enduring answers exist for a key set of questions, such as:

- Are nuclear weapons necessary for US deterrence and assurance strategies?
- If so, how many and what types are adequate for deterrence and assurance of whom against what?
- Are certain types or numbers of forces predictably "stabilizing" or "destabilizing"?
- What makes US deterrence strategies credible, and how important is the credibility of US threats?

Keith B. Payne, PhD, is president of the National Institute for Public Policy and professor and head of the Graduate Department of Defense and Strategic Studies at Missouri State University (Washington campus). He served as a deputy assistant secretary of defense and as a member of the congressional commission on US strategic posture. His most recent book is *The Great American Gamble: Deterrence Policy and Theory from the Cold War to the Twenty-First Century* (2008). Dr. Payne received an AB (honors) in political science from UC Berkeley and a PhD (with distinction) from the University of Southern California.

At the risk of shattering widespread illusions, it is important to understand an inconvenient truth: there is no basis for confident, definitive answers to any of these fundamental questions. All attempts to answer these questions involve considerable speculation. And no answer, however insightful for the moment, can be considered pertinent across time and place.

Why? Because deterrence is not a physical science; it is an arcane psychological art involving a shifting mosaic of adversary decision makers, circumstances, uncertainty, and error. There is considerable inherent uncertainty and unavoidable ambiguity in the functioning of deterrence, because predicting foreign decision making—particularly under stressful conditions—is an inherently uncertain business. As the Obama administration's director of central intelligence Leon Panetta recently observed, "Our biggest problem is always how do we get into the head of somebody . . . Those are the kinds of things that are obviously very tough for intelligence to predict."[2] James Clapper, the director of national intelligence, similarly observed, "We are not clairvoyant."[3]

Humility—not hubris—should govern all our discussions, claims, and expectations of deterrence, because it fundamentally is about getting "into the head" of foreign decision makers. We may have some confidence in our capability to know how many weapons of varying types are required to hold different sets of opponents' targets at risk (although even here there are uncertainties). Despite the fact that opponent vulnerability has historically been the focus of confidence regarding deterrence,[4] the character of forces and related calculations about the vulnerability of opponents' targets do not tell us whether or how deterrence will function. The capability to threaten targets is only one in a very long list of factors contributing to this psychological art.

For example, the number of our weapons and our related capability to threaten specific target sets will mean little or nothing for deterrence unless the opponent also

- understands US threats and communications;
- values greatly the types of targets the US can threaten;
- links the US threat to some specific act it must not undertake;
- makes decisions per an informed calculation of estimated costs and benefits;
- is not driven by some internal or external imperative to act despite the US threat;

- believes, to some degree, that the US threat would be executed if it does not comply and would not be executed if it does comply;
- fears the US threat more than it fears conciliation over the issue in question;
- deems conciliation to be a tolerable act; and
- has positive control over its own actions and forces.

Note that these and many other factors determining the process of deterrence have as much to do with an opponent's unique perceptions, values, culture, and decision-making process as with the numbers and types of forces we may have. Opponents' internal characteristics and circumstances vary widely and can literally determine the functioning of deterrence—whatever the nature of US capabilities and warnings. Thus, on any given occasion, the deterrence value or effect of a particular type of US threat can range from zero to all-important, and the correlation between deterrence effect and numbers and types of forces can vary greatly and unpredictably. Consequently, there can be no confident generalizations that a specific deterrence effect will follow from some given number of nuclear weapons or force structure.

Nevertheless, noted commentators frequently offer heroically confident claims that deterrence will function reliably and predictably and will do so at some general or specific low number of nuclear weapons. These claims typically come without reference to the particular action to be deterred or any apparent examination of the context, the stakes, or the opponents' circumstances or unique decision-making character.[5] To wit:

- "A total stockpile on the order of 500 warheads would satisfy the principle objectives of strategic nuclear deterrence in 'rational' scenarios where strategic deterrence is a useful concept."[6]
- "Deterring Russia, as well as China and other states that have acquired nuclear weapons, remains a justifiable function of U.S. nuclear weapons policy. But several thousand U.S. nuclear warheads are not needed to discharge that mission; a few hundred would suffice."[7]
- "The United States needs relatively few warheads to deter China. A limited and highly accurate U.S. attack on China's 20 long-range ballistic missiles would result in as many as 11 million casualties."[8]

- " . . . a few hundred warheads, are more than adequate to serve as a deterrent against anyone unwise enough to attack the United States with nuclear weapons."[9]
- "We estimate that a U.S. strategic force of some 500 operationally deployed warheads would be more than adequate for deterrence."[10]
- "Deterrence would remain robust with far smaller arsenals on far lower levels of alert. The United States and Russia should aim to cut the numbers of their nuclear weapons to the low hundreds."[11]
- "No sane adversary would believe that any political or military advantage would be worth a significant risk of the destruction of his own society . . . Thus ten to one hundred survivable warheads should be more than enough to deter any rational leader from ordering an attack on the cities of the United States or its allies."[12]
- "Having 100 nuclear warheads . . . will deter others from using nuclear, biological, or chemical weapons or from even engaging in conventional attacks."[13]
- "From a practical perspective, several second-strike nuclear weapons are more than enough to keep the most aggressive adversary at bay."[14]
- "'Extended deterrence' does not have to mean 'extended nuclear deterrence.' United States conventional capability, when combined with that of each of the allies in question, constitutes a deterrent to any conceivable aggressor at least as credible as that posed by its nuclear weapons."[15]

There is a near-endless supply of such promises that relatively few US nuclear weapons surely will be adequate to deter or that nonnuclear deterrence will be adequate. These promises typically are offered up as if the precise functioning of deterrence follows a predictable formula: the stakes involved in future crises already are well-known, and all future opponents have the necessary perceptions, goals, motivations, values, determination, culture, governing worldview, and mode of communication and decision making. On the basis of this presumption regarding context, opponent perceptions, and decision making, confident promises are made that some specific level or type of US force surely will deter or that some types of forces predictably will be "stabilizing" or "destabilizing."

The attractiveness of this type of thinking is its convenience and comfort. It avoids the truly hard work of trying to understand opponents and how they may perceive and react to US deterrence strategies and, thus,

how those strategies might actually work. It also facilitates the deceptively comforting conclusion that nearly all severe threats can be deterred reliably and predictably with minimal effort because all rational opponents surely will perceive our deterrence pronouncements properly, calculate their own interests predictably, and respond as necessary for our deterrence strategies to work. In other words, they will not dare strike us: "No regime, no matter how aggressive and risk-inclined, would be so foolish as to attack the United States, a move that would yield little advantage, and thereby incur an attack's clear consequence—utter destruction."[16] Seemingly everybody knows that opponents will think and behave in this fashion, and thus deterrence will work predictably and universally: "One advantage of deterrence is that it induces responsible behavior by enemies as a matter of their own self-interest. Even dictators tend to put certain basic interests above all else—preeminently their survival in power . . . Aggression becomes unattractive if the price is devastation at home and possible removal from power . . . *The logic of deterrence transcends any particular era or enemy*"[17] (emphasis added).

The problem with this convenient, comforting narrative is that American observers neither control nor often understand how opponents will perceive deterrence threats or what will constitute "rational" decision making and behavior according to their Weltanschauung. While the presumed decision making and behavior might take place on a given occasion, on other occasions a very different set of principles may govern opponent perceptions and decision making—hence, the great uncertainties surrounding the functioning of deterrence. In short, the world is made up of polities with dramatically varying worldviews, sources of inspiration and information, and modes of decision making. That variation can affect decisively whether and how deterrence functions and whether some particular force could be adequate for deterrence, stabilizing or destabilizing.

Numerous historical cases exist of regimes whose crisis decision making and behaviors strayed well beyond the bounds of rationality assumed by those offering precise, convenient, and comforting claims that deterrence will function predictably. Prime examples include:

- Hitler in his bunker in 1945 willfully contributing to the destruction of Germany;
- Mao Zedong in 1958 ordering the shelling of Quemoy island for the purpose of eliciting US nuclear threats;

- Cuba's leaders in 1962 demanding that their Soviet patrons launch a nuclear war against the United States;
- Nikita Khrushchev in1962 moving missiles to Cuba with the comment, "They can attack us and we shall respond. This may end in a big war";[18]
- Arab state leaders in 1973 launching a massive armored attack on Israel, a putative nuclear power; and,
- Saddam Hussein in 1991 raining missile attacks on Israel, even reportedly against the Dimona nuclear reactor, in the hope of provoking war with Israel.

There are, of course, explanations of sorts for all of these choices, but these explanations move quickly beyond the model of prudent, informed, and self-interested calculations assumed by those making confident promises about the functioning of deterrence. Prospectively, one may add to this list Iranian president Mahmoud Ahmadinejad, who claims confidence in divine protection and that he was "surrounded by a halo of light" when he addressed the UN in 2005.[19]

Former director of central intelligence George Tenet captured the point here with his observation, "What we believe to be implausible often has nothing to do with how a foreign culture might act."[20] The repeated confident claims that all opponents are sure to perceive and calculate predictably—as is necessary for deterrence to work at some specified low force level—typically either ignore, or deny, the importance of the profound variation in worldviews and decision making. As such, these claims are worse than empty; they are misleading and thus potentially dangerous.

These types of claims are a legacy of the fact that deterrence theory in the United States has been highly abstract for decades. Politically attractive promises that deterrence is sure to work at some specific, much lower, nuclear force level are derived from supposedly universal principles that govern all rational leadership decision making: they will calculate and conciliate predictably because their rationality and our threat will leave them no other option. Armed with this presumption of what constitutes rational behavior, confident claims are made, such as those noted above, that deterrence will function, with little apparent recognition or knowledge of the unique factors that can govern opponents' decision making. If these universal principles apply to all rational decision making, then deterrence

can be expected to function according to predictable rules, and there is little need to understand the specific opponent in detail.

In fact, however, the meaning of *rational* underlying these deterrence claims typically consists of those behaviors and modes of decision making that seem reasonable or sensible to those making the claims.[21] Deterrence is supposed to work reliably because even small numbers of nuclear weapons can pose a fearsome threat, and leaders will be rational qua reasonable in response. Thus, they will surely perceive and count costs, as necessary for deterrence to work: "In a nuclear world any state will be deterred by another state's second-strike [retaliatory] forces. One need not become preoccupied with the characteristics of the state that is to be deterred or scrutinize its leaders."[22] And, "Not much is required to deter. . . . Because the use of nuclear weapons could lead to catastrophe for all of the parties involved, nuclear weapons create their own credibility."[23]

Such confident and near-universal claims that we should expect deterrence to function predictably at relatively low numbers of US nuclear forces—whether 300, 500, or 1,000—seemingly know how opponents will perceive US deterrence threats, value the stakes at risk, calculate costs and benefits, and make and implement decisions. Yet, these comforting promises should not be taken seriously; they reflect hubris and the appearance of, rather than the reality of, such knowledge. It simply is not possible in practice, as opposed to a Gedanken experiment, to identify and understand the interaction of the factors that can drive opponents' deterrence decision making so precisely. The fact that such predictions cannot be made with confidence obviously does not prevent the widespread practice.

Lawrence Freedman makes this point with his wry comment that deterrence theory is a "gift to strategists in that its nature and workings remain so elusive and so imperfectly understood as to permit endless speculation with little danger of empirical refutation."[24] There is, however, a severe downside to this "gift." The lack of accountability and discipline gives license to an abundance of confident assertions from within and outside government that US deterrence strategies will be effective with ever fewer or no US nuclear weapons. These comforting claims usually come with trappings of precision and analytical rigor, when in fact they cannot be other than extremely speculative. Unless the unique decision-making parameters of opponents are considered in context, there is little basis for claims for any particular occasion about what is likely to prove adequate for deterrence or what will be stabilizing or destabilizing.

With that fundamental caveat firmly in mind, we can examine with appropriate humility the question of whether or not nuclear deterrence is an important element in US and allied security. And, if so, how many and what types of nuclear weapons are adequate for this purpose?

To the extent that an informed, reasoned answer to the lead question is possible, my necessarily nuanced answer is yes—at this particular time, nuclear deterrence should be deemed critical for US and allied security. For some plausible threats, to paraphrase Frederick the Great, deterrence without nuclear weapons is like an orchestra without instruments. It can produce noise but probably not the desired music.

In offering this answer I am not claiming to know that in all or any future occasions, deterring attack will require credible nuclear deterrence or that deterrence will even be possible. As noted above, many factors go into the functioning of deterrence. And, there are other potentially important tools for deterrence, including nonnuclear and nonmilitary. By the same token, however, no one can claim with any honesty to know that nonnuclear deterrence will be adequate on some future occasions, possibly including an existential threat to the United States and its allies.

Fortunately, by introducing some evidence into this discussion, we can move beyond competing speculation that nuclear weapons will or will not be important for deterrence. My conclusion that credible nuclear deterrence is important for the United States follows from three basic empirical reference points:

1. Nuclear deterrence appears to have been key to deterrence functioning on critical occasions during the Cold War and since. Further, I see zero evidence to suggest that nuclear deterrence could not again be key to deterrence working on some critical future occasions. As Mark Twain said, "The past may not repeat itself, but it sure does rhyme."
2. In the contemporary era, the consequences of a single significant failure of deterrence are potentially so catastrophic for society that we need deterrence strategies that are as effective as possible; nuclear deterrence cannot ensure their functioning, but we should avoid the risk of their failing for the lack of credible nuclear deterrence.
3. Our great need for credible deterrence corresponds directly to our general societal vulnerability to WMD attacks. We should ever seek effective deterrence strategies, but they are particularly needed when we are so ill prepared to protect civil society against even relatively

> limited WMD strikes. As William Perry, Ashton Carter, and Michael May observed with regard to the detonation of a single nuclear weapon in a US city, "The scale of disaster would quickly overwhelm even the most prepared city and state governments."[25] The unfortunate level of US vulnerability could change, but until then our deterrence strategies must be as effective as possible, and if the past is precedent, credible nuclear deterrence will have an essential role to play.

Conventional deterrence has been manifestly effective on occasion, but it also has an unfortunate 2,000-year record of periodically failing catastrophically: most recently, there were no nuclear weapons to deter war in 1914 and 1939. What followed were approximately 110 million casualties in fewer than 10 combined years of warfare. The subsequent 6-1/2 nuclear decades compare very favorably to that horrific prenuclear record. Nobel laureate Thomas Schelling makes the material point simply: "One might hope that major war could not happen in a world without nuclear weapons, but it always did."[26] Indeed, we have already been to the "nuclear zero mountaintop."

Nuclear deterrence has helped to prevent a repeat of such horrors. In a comprehensive examination of the US–Soviet historical record, Ned Lebow and Janice Stein conclude: "The reality of nuclear deterrence had a restraining effect on both Kennedy and Khrushchev in 1962 and on Brezhnev in 1973. When Superpower leaders believed that they were approaching the brink of war, fear of war pulled them back."[27] And, "The history of the Cold War suggests that nuclear deterrence should be viewed as a powerful but very dangerous medicine . . . As with any medicine, the key to successful deterrence is to administer correctly the proper dosage."[28] Yes, indeed.

There is similar evidence from the post–Cold War era. In 2009, for example, former Indian army chief Gen Shankar Roychowdhury asked: "Do nuclear weapons deter?" He then answered his own question based on the empirical evidence, "Of course, they do. Pakistan's nuclear weapons deterred India from attacking that country after the Mumbai strikes. . . . It was due to Pakistan's possession of nuclear weapons that India stopped short of a military retaliation following the attack on Parliament in 2001."[29] Here we have India's army chief explaining precisely what deterred India on two occasions—Pakistan's nuclear deterrent.

The first Gulf War also offers evidence of the value of nuclear deterrence. It appears that the US nuclear deterrence strategy was key to deterring the Iraqi use of WMD in the war. In August 1995, the former Iraqi foreign minister, Tariq Aziz, said that Iraq was deterred from using its

WMD because the Iraqi leadership had interpreted Washington's threats of grievous retaliation as meaning nuclear retaliation.[30]

In January 1996, former head of Iraqi military intelligence Gen Wafic al Sammarai said: "Some of the Scud missiles were loaded with chemical warheads, but they were not used . . . the warning was quite severe, and quite effective. The allied troops were certain to use nuclear arms, and the price will be too dear and too high."[31]

Gen Hussein Kamal, Iraqi minister of military industry and Saddam Hussein's son-in-law, said in 1995: "During the Gulf War . . . there was no decision to use chemical weapons for fear of retaliation. They realized that if chemical weapons were used, retaliation would be nuclear."[32]

These few references do not close this case—historical studies rarely are settled definitively. Saddam Hussein himself once said that "Iraq did not use WMD during the 1991 Gulf War as its sovereignty was not threatened."[33] This explanation is not necessarily inconsistent with the deterrence explanation, and discerning the truth in his various statements undoubtedly poses a challenge—during these same interrogations he also said that he invaded Kuwait because the Kuwaiti leader had told a crude joke about Iraqi women.[34]

At this point, the most informed, unclassified analyses of the first Gulf War conclude that Saddam Hussein was indeed deterred from chemical and biological weapons (CBW) employment by his fear of US nuclear retaliation. For example, Charles Duelfer, executive deputy chairman of the UN Special Commission on Iraq, has testified that "The Iraqis did not use these weapons even when they were losing, and I asked them why, and the long and the short of it was that Saddam thought that he would not survive. So the [deterrence] message worked. Saddam was deterred."[35] Equally important, well-informed analyses also conclude that other possible nonnuclear deterrence threats, such as regime change, were not sufficiently credible to deter Saddam Hussein.

In short, while conventional deterrence may well be adequate on some or many future occasions, there is sufficient historical evidence available to demonstrate that nuclear deterrence has helped to prevent conflict or escalation in the past. It also suggests that, in the absence of some significant transformation, the absence of credible nuclear threats would increase the risk of deterrence failure in some future cases.

This deterrent value of nuclear threats may be of increasing importance as chemical and biological weapons become potentially more lethal and

more easily acquired; the undeterred use of CBW could destroy the fabric of society, without nuclear use. This is why the elimination of nuclear weapons would not eliminate catastrophic threats to civilization, but would preclude nuclear deterrence from helping to counter such threats. The "mountaintop" vision of "nuclear zero" may well include the dark potential of leaving unprotected civilians more vulnerable to CBW attack.

One reason why nuclear threats contribute to the functioning of deterrence appears to be because they can help to reduce the chances that opponents will be so optimistic about their circumstances, so committed to their goals, or so cost-tolerant that they will accept or ignore the risks of defying our deterrence threats. There is a deeply ingrained human cognitive drive to believe and interpret information in ways consistent with one's established desires and preferred facts, despite contrary evidence. This can cause opponents to discount or deny deterrent threats that we believe should be sufficient and credible. On this basis, they undertake high-risk gambits that defy our sense of reason, and deterrence can fail unexpectedly as a result. This is not necessarily a matter of an opponent's rationality but the fragility of perceptions, judgments, and imprudence. The self-serving hope, of course, is that no opposing leader will be so optimistic, committed, cost-tolerant, or imprudent, and, thus, all opponents will be predictably deterred. Unfortunately, history does not warrant such a hope.[36]

While US nuclear deterrence cannot close down these well-traveled avenues to deterrence uncertainty, we do know that it can moderate an adversary's otherwise unduly sanguine perceptions, expectations, and calculations and thereby strengthen US deterrence strategies. As Alexander George and Richard Smoke concluded in 1974 based on their case studies, an opponent's belief that the risks of provocation are incalculable or uncontrollable can provide the basis for deterrence success.[37] The cases I have cited appear to illustrate this deterring effect of nuclear weapons.

Can we be certain that nuclear deterrence always will perform as we hope? Of course not. But, do we want to run the potential risk of degrading deterrence by taking our credible nuclear threats off the table? Again, my answer is, of course not. The bipartisan Congressional Strategic Posture Commission reached the same answer and specifically endorsed the maintenance of credible US nuclear escalation threats, as did the Obama administration's generally commendable 2010 Nuclear Posture Review.

I would like to comment on the key word *credible* in discussions of deterrence. The importance of deterrence credibility and how threats may be

made credibly have been questions at the heart of our nuclear debates for decades. Different nuclear policy positions often have their origin in different presumptions about credibility.

For example, in the 1960s Herman Kahn insisted that a high level of credibility is essential for US deterrence strategies and that the US capability to defend society against nuclear attack is necessary for credible US extended deterrence. He reasoned that if we ourselves are vulnerable to destruction, then our deterrence threats on behalf of others are unlikely to be credible. This is why he advocated so strongly for US missile defense and civil defense, even when doing so was extremely unfashionable.

In contrast, Thomas Schelling insisted that Kahn overstated the need for logical deterrence credibility and that defending US society against attack is unnecessary for extended deterrence. In fact, he suggested that thick missile defense could undercut deterrence.[38]

Which position was correct? The answer is that both probably were correct under different circumstances. In some plausible contexts and cases, deterrence credibility would likely benefit greatly from US defensive capabilities; in other plausible cases, deterrence likely will function as we hope, even in the absence of US societal defenses. In still other cases, moreover, US defenses may be wholly irrelevant to the credibility of deterrence, but they may be essential for the protection of society when deterrence fails—and if history is any guide, it periodically will fail.

My point here is that the level of credibility necessary for deterrence to work can vary by opponent and context, as can the measures necessary to make threats credible. In each contingency, the details of leadership, personality, time, place, stakes, culture, ideology, religion, and communication can shape the credibility opponents attribute to US deterrence threats and the steps we might take to strengthen that credibility and, thus, deterrence.

Consequently, because we care about credible deterrence, there is no substitute for understanding opponents to the extent possible so that we can adapt our deterrence strategies to the unique requirements of each contingency. With enough serious analysis and smart policy choices, we can and must establish deterrence strategies and related force requirements that can be adapted to diverse opponents and contexts. Otherwise, our deterrence strategies will rely to a large extent on good fortune. And, as many have noted in the past, luck is not good strategy.

Given the great variation possible in the requirements for credible deterrence, the most obviously important US force structure characteristic

for deterrence is not the size of our forces, per se, but their flexibility and resilience—*flexibility* meaning US possession of a spectrum of possible threat options suitable for a wide range of opponents and contingencies, and *resilience* meaning the capability to adapt deterrence to changes in threats and contexts, including rapid and unanticipated changes.

The bipartisan Congressional Strategic Posture Commission did not try to identify "the" minimum number of nuclear weapons necessary for deterrence and assurance.[39] This deliberate omission recognized the fact that these force requirements can change rapidly because they are driven by many fluid factors, including unpredictable developments in the threats we and our allies face.[40] Any specific number of weapons we might have identified as "just right" at the time for deterrence and assurance could have become wholly inappropriate shortly thereafter.

Rather than selecting an inherently uncertain and transient "right" number of nuclear weapons for deterrence, the commission highlighted the need for a flexible and resilient force posture to support deterrence and assurance across a fluid and shifting landscape of threats and contexts.[41] The basic logic is that US capabilities and strategies for deterrence and assurance must be able to adapt rapidly to changing threats.

The commission's emphasis on the need for flexibility in our force posture was not new; it harkens back to the Schlesinger Doctrine of 1974 and to the 1980 "Countervailing Strategy" of the Carter administration.[42] The US Strategic Command's 2006 *Deterrence Operations Joint Operating Concept* similarly emphasizes the need for flexibility in the US force posture for credible deterrence, as did the 1994 and 2001 Nuclear Posture Reviews.[43] Indeed, the requirement for these force characteristics is one of the long-standing continuities of US strategic policy.[44] The commission noted in particular that the importance of flexibility and resilience will increase as US forces decline in numbers.[45]

This emphasis on the value of flexibility and resilience for deterrence is the primary reason the commission recommended that the administration maintain the strategic triad of bombers, ICBMs, and sea-based missiles. Each of the three separate triad "legs" can contribute significantly to the overall flexibility and resilience of our forces.[46] In recognition of the fact that deterrence is uncertain and may prove unreliable, the commission also rightly concluded that the United States must design its strategic forces to help defend against attack if deterrence fails and that missile defense be considered an integral part of the US strategic force posture.[47]

There is no basis for identifying "the" right number of nuclear weapons for the purposes of deterrence, but there is a correlation between an arsenal's numbers and the deterrence advantages provided by force flexibility and resilience. As nineteenth-century German philosopher George Hegel observed, quantity becomes quality. In this case, a large, diverse strategic arsenal should provide greater flexibility and resilience than a smaller arsenal, and a diverse strategic triad of forces should be superior in this regard to a dyad or monad.

The disadvantage of a small, less-diverse force structure is that it may be too inflexible and limited to contribute as needed to some US deterrence goals. For example, a small force is likely to offer fewer choices among warheads and delivery modes, thereby limiting US threat options. And, it is less likely to compensate for weaknesses in one area by strengths in another area. That is why the bipartisan Strategic Posture Commission endorsed US maintenance of a diverse US strategic triad for deterrence, as did the 2010 Nuclear Posture Review—they got it right.

A relatively small, inflexible US force would also ease the technical/strategic challenges for opponents who might seek to counter or otherwise get around our deterrence strategies in the future. It could thereby actually encourage opponents to compete and challenge our deterrence strategies. If so, the lack of flexibility and resilience could provide us with too little capacity to respond as necessary to maintain credible deterrence strategies in the face of surprises and dangerous political and/or technical developments.

This potential lack of a safety margin at low force levels is, perhaps, why proponents of a "glide path" to deep reductions in US nuclear capabilities typically assume the existence and continuation of a relatively benign threat environment.[48] This is an unwarranted, overly optimistic planning assumption: international political relations can deteriorate rapidly, and severe threats can wax much more rapidly than our capability to adapt—particularly if our forces and infrastructure lack flexibility and resilience.

As we move forward for arms control purposes to reduced numbers of nuclear launchers and warheads, our priority for credible deterrence should be to preserve as much flexibility and resilience as is possible given the reductions mandated. As numbers decline, the force structure allowed needs to be optimized for flexibility and resilience to avoid the degradation of deterrence that a smaller force may otherwise cause. Indeed, we should be keen to avoid numeric reductions that could degrade credible deterrence by overly constraining the flexibility and resilience of our forces and related defense infrastructure.

Recognition of this guideline should help us to focus less on the mechanistic quest for parity with Russia at ever-lower numbers as the priority goal of US nuclear policy and to focus more on the deterrence value of force structure flexibility and resilience. These are the force attributes to maintain, given their potential contribution to credible deterrence and our continuing great need for deterrence.

Will adequate flexibility and resilience ensure deterrence? Of course not; nothing can do that. But it should reduce the risk that deterrence will fail because we do not have the threat options suitable for the occasion. Correspondingly, it can help to assure allies who rely on the US nuclear umbrella and may otherwise fear that the degradation of US deterrent capabilities endangers their own security. These fears could lead some allies and friends to reconsider their own need for nuclear weapons and thereby promote nuclear proliferation. We already see this dynamic in play among some allies.[49]

It is useful to close with the observation that our preferred force numbers and types should follow the demands of strategy, not the reverse. This is no less true when that strategy is deterrence. Credible deterrence is a precious product that defies easy or precise prediction. But, we do know that in the past, nuclear deterrence contributed to preventing conflict or escalation, and it may be necessary to do so again when we face severe risks. Consequently, the maintenance of credible nuclear deterrence should continue to be a national priority.

In addition, the requirements for credible deterrence are many and will vary more or less for each different opponent and contingency. Given this variation, the risks of a small and inflexible force structure may be severe when US deterrence needs and goals are wide ranging. Instead, we should maintain a force structure, including a nuclear arsenal of the size and diversity necessary for flexibility and resilience. Why? Because these characteristics are likely to be advantageous for deterrence on at least some occasions, and effective deterrence at those times may be essential to US and allied survival. SSQ

Notes

1. William J. Perry et al., *America's Strategic Posture* (Washington: US Institute of Peace Press, 2009), 13, 17, 21.

2. Leon Panetta, testimony before the House Permanent Select Committee on Intelligence, Worldwide Threats Hearing, 10 February 2011.

3. Senate Select Committee on Intelligence Hearing—*Statement for the Record by Director of National Intelligence James R. Clapper—Worldwide Threat Assessment of the United States Intelligence Community*, 16 February 2011.

4. Most recently see James Wood Forsyth Jr., B. Chance Saltzman, and Gary Schaub Jr., "Minimum Deterrence and its Critics," *Strategic Studies Quarterly* 4, no. 4 (Winter 2010): 3–12.

5. For example, Hans Kristensen, Robert Norris, and Ivan Oelrich, *From Counterforce to Minimal Deterrence: A New Nuclear Policy on the Path Toward Eliminating Nuclear Weapons, Federation of American Scientists and the Natural Resources Defense Council*, Occasional Paper no. 7 (April 2009), 43; and Daryl G. Kimball, "Reassessing the Role of Nuclear Weapons," *Arms Control Today* 39, no. 1 (January/February 2009), http://www.armscontrol.org/act/2009_01-02/Focus.

6. Jeff Richardson, "Shifting From a Nuclear Triad to a Nuclear Dyad," *Bulletin of the Atomic Scientists* (September/October 2009): 40.

7. Wolfgang Panofsky, "Nuclear Insecurity: Correcting Washington's Dangerous Posture," *Foreign Affairs* 86, no. 5 (September/October 2007): 113.

8. Natural Resources Defense Council, "Pentagon Is Exaggerating China's Nuclear Capability to Justify Buying New Generation of U.S. Weapons, Report Finds," press release, 30 November 2006.

9. Kristensen, Norris, and Oelrich, *From Counterforce to Minimal Deterrence*, 2.

10. Sidney D. Drell and James E. Goodby, *What Are Nuclear Weapons For? Recommendations for Restructuring U.S. Strategic Nuclear Forces*, Arms Control Association report (revised October 2007), 15.

11. Bruce Blair, "Trapped in the Nuclear Math," *New York Times*, 12 June 2000.

12. Steve Fetter, "Nuclear Strategy and Targeting Doctrine," in *The Nuclear Turning Point*, ed. Harold A. Feiveson (Washington: Brookings Institution Press, 1999), 57.

13. Morton Halperin et al., "Parsing the Nuclear Posture Review," *Arms Control Today* 32, no. 2 (March 2002): 19–20.

14. Forsyth, Saltzman, and Schaub, "Minimum Deterrence and Its Critics," 7.

15. Gareth Evans and Yoriko Kawaguchi, *Eliminating Nuclear Threats: A Practical Agenda for Global Policymakers*, Report of the International Commission On Nuclear Nonproliferation and Disarmament (Canberra: ICNND, 2009), 66.

16. Elbridge Colby, "Restoring Deterrence," *Orbis* 51, no. 3 (Summer 2007): 419.

17. "In Defense of Deterrence," *New York Times*, 10 September 2002, A-24.

18. Quoted in Aleksandr Fursenko and Timothy Naftali, *One Hell of a Gamble: Khrushchev, Castro and Kennedy, 1958–1964* (New York: W. W. Norton and Co., 1997), 241.

19. See the discussion in Keith B. Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century* (Fairfax, VA: National Institute Press, 2008), 216, 349–50.

20. George Tenet (with Bill Harlow), *At the Center of the Storm: My Years at the CIA* (New York: HarperCollins, 2007), 46.

21. As discussed in Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: University Press of Kentucky, 1996), 56–58.

22. Kenneth N. Waltz, "Nuclear Myths and Political Realities," *American Political Science Review* 84, no. 3 (September 1990): 737–38.

23. Kenneth N. Waltz, "More May Be Better," in *The Spread of Nuclear Weapons*, eds. Scott D. Sagan and Kenneth N. Waltz (New York: W. W. Norton, 2003), 22, 26.

24. Lawrence Freedman, "The Rationale for Medium-Sized Deterrent Forces," in *The Future of Strategic Deterrence*, ed. Christopher Bertram (Hamden, CT: Archon, 1981), 52.

25. William J. Perry, Ashton B. Carter, and Michael M. May, "After the Bomb," *New York Times*, 12 June 2007. See also Jerry Seper, "Justice Department lacking a WMD response," *Washington Times*, 1 June 2010, http://www.washingtontimes.com/News/2010/jun/1/justice-department-lacking-a-wmd-response/?page=2.

26. Thomas Schelling, "A World Without Nuclear Weapons?" *Daedalus* (Fall 2009): 125.

27. Ned Lebow and Janice Stein, *We All Lost the Cold War* (Princeton, NJ: Princeton University Press, 1994), 356.

28. Ibid., 368.

29. Quoted in "Pak's N-bomb Prevented India from Attacking it after 26/11," Department of State, *ISN News*, 10 March 2009.

30. As discussed in R. Jeffrey Smith, "U.N. Says Iraqis Prepared Germ Weapons," *Washington Post*, 26 August 1995, A-1.

31. Statement by Gen Wafic al Sammarai in "Frontline no. 1407: The Gulf War, Part I," 9 January 1996, transcript, 12. See also the statements by General al Sammarai in "Frontline: The Gulf War, Parts

I and II," 9–10 January 1996. Comprehensive background interviews are available at www.wgbh.org. See also Tim Trevan, "Inside Saddam's Death Lab," *Sunday Times* (London), 14 February 1999, www .sunday-times.co.uk/news/pages/sti/99/02/4; and Tim Trevan, *Saddam's Secrets: The Hunt for Iraq's Hidden Weapons* (North Pomfret, VT: HarperCollins, 1999), 45.

32. Quoted in Gen Hussein Kamal UNSCOM/IAEA briefing, 22 August 1995, Amman, Jordan.

33. Casual conversation between Saddam Hussein and George L. Piro, Baghdad Operations Center, 13 May 2004, FBI memo, 2, http://foia2.fbi.gov/husseinsaddam/written_interviews.pdf.

34. Saddam Hussein to US interrogator George Piro. See "Interrogator Shares Saddam's Confessions: Tells 60 Minutes Former Iraqi Dictator Didn't Expect U.S. Invasion," *CBS News*, 27 January 2008, http://www.cbsnews.com/stories/2008/01/24/60minutes/mains37494.shtml.

35. Charles A. Duelfer, testimony, Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities: "The Weapons of Mass Destruction Program of Iraq," S. Hrg. 107-573, 107th Cong., 2d sess. (Washington: GPO, 2002), 92–93, http://frwebgate.access.gpo.gov/cgi-bin /getdoc.cgi?dbname=107_senate_hearings&docid=f:80791.pdf. See also the work by Kevin Woods, task leader of the Iraqi Perspectives Project at the Institute for Defense Analysis, and David Palkki, deputy director of National Defense University's Conflict Records Research Center. They presented their respective views on this subject at a policy forum luncheon by the Washington Institute for Near East Policy, "Knowing the Enemy: Iraqi Decision Making under Saddam Hussein," 20 September 2010. This forum can be found at http://www.c-spanarchives.org/program/id/233237.

36. See Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: University Press of Kentucky, 2001), 1–15, 39–77. Barry Wolf's *When the Weak Attack the Strong: Failures of Deterrence* (RAND, 1991) chronicles numerous examples of high-risk actions by leaders who—based on any reasonable standard—should have been deterred.

37. As Alexander George and Richard Smoke observed in 1974 based on their case studies, an opponent's belief that the risks of provocation are not calculable or controllable "is usually a sufficient condition for deterrence success." George and Smoke, *Deterrence in American Foreign Policy* (New York: Columbia University Press, 1974), 529.

38 See the discussion in Payne, *Great American Gamble*, chaps. 1 and 2.

39. Perry et al., *America's Strategic Posture*, 17.

40. Ibid., 23–24.

41. Ibid., 22–23, 29.

42. See the discussion in Payne, *Great American Gamble*, chap. 5.

43. US Strategic Command, *Deterrence Operations Joint Operating Concept*, version 2.0, December 2006, 3, 8, 17, 40. See also "Nuclear Posture Review" from the 1995 Secretary of Defense Annual Report to Congress, http://www.dod.mil/execsec/adr95/npr_.html.

44. See Kurt Guthe, *Ten Continuities in U.S. Nuclear Weapons Policy, Strategy, Plans, and Forces* (Fairfax, VA: National Institute for Public Policy, 2008), http://nipp.org/Publication /Downloads/Publication%20Archive%20PDF/N-Continuities%20Draft_Rev%202.1.pdf.

45. Perry et al., *America's Strategic Posture*, 26.

46. Ibid., 25–26, 29.

47. Ibid., 23.

48. For example, "The analysis of the effect of deep reductions on international security is built upon three main assumptions. Firstly, it is assumed that international relations (both between Russia and the US and with their potential adversaries) will not get significantly better or worse than they are today." James Acton, *Deterrence During Disarmament: Deep Nuclear Reductions and International Security*, Adelphi Papers 417 (London: Routledge Online Publication, March 2011), 22.

49. See, for example, Tom Scheber and Kurt Guthe, *U.S. Extended Deterrence and Assurance for Allies in Northeast Asia* (Fairfax, VA: National Institute Press, 2010).

Deterrence at the Operational Level of War

James Blackwell

Let us not make the world safe for conventional war.

—Michael Quinlan, *Thinking About Nuclear Weapons*

Deterrence was a strategy of the Cold War. It guided the development of strategic concepts even when nonnuclear operations were the predominant concern of the US military, including conventional warfare in Korea and Europe and counterinsurgency in Southeast Asia.

Today our understanding of deterrence has atrophied. In fact, deterrence has been incarcerated into one of two holding cells, as if it were some kind of contagion that requires quarantine. For all operations that might involve employment of nuclear weapons, campaign planning has become the exclusive jurisdiction of US Strategic Command (STRATCOM). Even there, deterrence is but one of six missions.[1] For the geographic combatant commands, deterrence is confined to one phase of a joint campaign, one that is most often more hope than plan. Phase 2 of the joint campaign, "Deterrence," has in fact become mostly all about moving forces into the theater for the purpose of seizing the initiative or mounting a defense rather than deterring the conflict from happening altogether.

This conceptual decline occurred for no apparent reasons. In the 1990s, many became convinced that our conventional combat power was so superior we did not need nuclear weapons to deter—conventional capabilities would be sufficient. Then in the beginning of the twenty-first century we became—rightly—focused on winning the war against violent extremists and conducting counterinsurgency campaigns.

Dr. James Blackwell is special advisor to the assistant chief of staff, strategic deterrence and nuclear integration, Headquarters, US Air Force. He received his PhD and MALD from the Fletcher School of International Law and Diplomacy and BS from the US Military Academy. He previously served as executive director of the Secretary of Defense Task Force on DoD Nuclear Weapons Management. He co-edited, with Barry Blechman, *Making Defense Reform Work* (Brassey's, 1990) and has also authored numerous books and articles.

In so many ways we now have deterrence all wrong—especially during campaign planning. For example, in the Joint Capabilities Integration and Development System (JCIDS) we combine deterrence capabilities with the force application joint capability area. As a result, platforms such as intercontinental ballistic missiles (ICBM), sea-launched ballistic missiles (SLBM), reentry vehicles and associated warheads, warhead arming, fusing and firing mechanisms, and long-range bombers—systems we hope never to use in nuclear combat—have to compete for resources with fighter aircraft, attack submarines, and MRAPs (mine resistant ambush protected vehicles) on the basis of military utility. This is a competition in which nuclear capabilities will never prove to be cost-effective to those who would rather fight than deter.[2]

It is time now to reinvent deterrence for the operational level of war in the twenty-first century. Deterrence is still about creating fear of consequences, but we have to apply military power to a vastly different world than the one in which the concept was created. Focusing on the concept of deterrence and its complexity is instructive at the operational level of war. Campaign planners should reconsider some fresh axioms for integrating deterrence.

The Concept of Deterrence

The deterrent value of nuclear weapons is inherent in the terrible nature of the destruction they can cause. Hence, the Joint Publication (JP) 1-02 definition of deterrence, "the prevention from action by fear of the consequences . . . a state of mind brought about by the existence of a credible threat of unacceptable counteraction," remains relevant for the twenty-first century. Indeed, the English word *deter* is derived from the Latin *de,* away from, and *terrere,* to frighten. One of the impenetrable basics of deterrence is the fundamental paradox that nuclear weapons exist never to be used. The reason for this paradox is in the basic physics of nuclear weapons. These things are not, as many have asserted, subsets of "kinetic" military capabilities. While distinct from nonkinetic capabilities, such as those in the cyber and space domains, nuclear weapons are certainly not simply more-powerful forms of classic firepower. Indeed the kinetic energy of a nuclear explosion, while orders of magnitude more powerful than that of an equivalent mass in a conventional weapon, is typically no more than half the total energy output of a nuclear device. The other half is distributed over thermal and radiation effects that no conventional munition can

generate. This is what sets them so far apart from other weapons in the history of human conflict.

Because nuclear weapons effects are so terrible, we must not blur the distinction between "nuclear" and "conventional" weapons, even if we feel compelled to create new categories for cyber, space, and informational effects that are "nonkinetic." Instead, we should explore how to integrate nuclear with conventional and nonkinetic capabilities into a new, comprehensive framework for deterrence.

Indeed, US STRATCOM's *Deterrence Operations Joint Operating Concept* (*DO JOC*) provides a framework for doing just that. The 2006 version of this document expands on JP 1-02 by asserting, "Deterrence operations convince adversaries not to take actions that threaten US vital interests by means of decisive influence over their decision making."[3] It suggests to planners that they can achieve decisive influence by credibly threatening to impose costs, deny benefits, and/or encourage restraint. The *DO JOC*'s purpose is to describe "how joint force commanders will conduct deterrence operations through 2025." It provides a necessary and useful framework for doing that within STRATCOM, but it is insufficient to guide the development, application, and employment of deterrence operational concepts among the geographic combatant commands or the development of deterrence capabilities by the services.

The Growing Complexity of Deterrence

Today, the context in which deterrence must be applied has grown so complex that the military must find ways to apply it at the operational level of war. We cannot leave it exclusively to academics and policymakers. Four global trends drive our understanding of deterrence at the operational level.

We Live In a Multipolar Nuclear World

According to the Carnegie Endowment for International Peace, there are nine nuclear-armed states (the United States, Russia, China, France, the United Kingdom, Israel, India, Pakistan, and North Korea).[4] This multipolar nuclear world will function systemically more like a balance-of-power world.

In a classic balance-of-power system, conflicts tend to be characterized by shifting coalitions rather than contending alliances. While this may mean that post–Cold War relationships among the United States, Russia,

and China are more likely to be stable in strategic terms, it may also mean that medium nuclear powers, such as France and India, will become key to future coalition relationships among the three larger nuclear powers. It may also mean that the United States will have to devote greater effort to building and maintaining strategic relationships since no single player can dominate the smallest coalition in a balance-of-power system. However, actions taken to deter one nuclear state will affect the others in complex ways that may present unforeseen dilemmas in dealing with a particular crisis.

For example, if a crisis between the United States and China were somehow to devolve into a conflict in East Asia and both sides maneuvered large military forces across the region, how would nuclear-armed India comprehend and interpret the various moves and countermoves? While India might be confident that neither the United States nor China would threaten it directly, the outcome of the crisis would have a profound effect on India's strategic interests. A risk-averse India would inexorably be drawn to the crisis and would find itself in a position of being solicited as the potential swing vote in terms of the weight of its own military power. This would not necessarily be explicit; it could quite easily take the form of precautionary mobilizations and movements of forces to deter China from taking advantage of opportunities to reengage in their long-standing border disputes. After all, China is the only nuclear power in history that has attacked another nuclear-armed opponent when it invaded Soviet territory in 1969. And how then would Pakistan respond to strategic actions by India? In some ways we may thus appear to be moving out of the twentieth century into the nineteenth.

We Also Now Live in a Proliferated Nuclear World

This means that lesser nuclear states and nonstates add increased risk of catalytic effects. Gone are the days when proliferation could be considered a good thing. The historic reasoning was if two countries were mutually deterred from going to war with each other by possession of nuclear weapons, then stability would increase as more countries acquired them. There would be fewer wars, and more countries would likewise be deterred. In reality, today's proliferated world is the opposite case, with the most immediate and extreme dangers being nuclear proliferation and nuclear terrorism.

Defiant proliferators seek nuclear weapons not to deter but to employ. At the same time, lesser nuclear states are much more likely to use the few nuclear weapons they possess.[5] In a conflict situation, once deterrence has

failed, lesser nuclear states' incentives are to use nuclear weapons first, before greater and medium powers remove them by other means. Once such an adversary initiates use of nuclear weapons, it is not likely to be restrained from further use of a limited arsenal, since there will be enormous pressure to use them or lose them.

Nuclear proliferators are also more risk-acceptant than responsible nuclear-armed states. They are more likely to adopt a first-use policy, to use all they have, and to provoke their use by others. Another complicating factor is coalitions of nuclear states. Coalitions of lesser nuclear states can disperse the effects of a response from a larger opponent and thus absorb more destruction and suffer more punishment than could a single larger nuclear state. Responsible nuclear powers must develop concepts of deterrence operations that will prevent such opponents from taking those risks by deterring the smaller power's use of nuclear weapons. US joint forces will therefore need new operational concepts for military capabilities to prevent such conflict and for operating on battlefields characterized by limited use of nuclear weapons.

The Behavioral Model of Deterrence Will Predominate

Cold War deterrence was built on the rational actor model, which emphasizes the intellectual nature of deterrence. It holds that the threat by an opponent to use nuclear weapons, resulting in sure destruction of the other, would be so risky that no one—regardless of cultural or behavioral attributes or institutional decision-making processes—would ever conclude they could prevail in such an ultimate nuclear contest. Bernard Brodie, Albert Wohlstetter, Herman Kahn, and Thomas Schelling are generally recognized as the intellectual founders of the rational actor school of deterrence.

Theorists developed many ways to conceptualize this objective calculus, from game theory to expected utility models. Each Cold War crisis has been analytically dissected, with the result that the United States and the Soviet Union developed mutual understanding of the limits of escalation and the "redlines" of crisis behavior and military action, though, as a result of post–Cold War assessments, many of these understandings are now demonstrably known to have been inaccurate. Widespread acceptance of the rational actor model resulted in a prevailing strategic deterrence orthodoxy of variations on the theory of "mutually assured destruction" (MAD), which today still commands widespread adherents. Journalist James Fallows famously characterized strategic deterrence concepts and related

arms control and defense policies based on the theory of MAD as akin to medieval theology.[6]

In contrast, the behavioral school emphasizes the cognitive nature of deterrence as applied to individuals, groups, organizations, and nations. A number of Cold War analysts recognized the psychological basis of deterrence. Robert Jervis, for example, argued that understanding each side's values, beliefs, and perceptions was necessary to comprehend their decision making. Ultimately, deterrence is in the mind of the deterred. Thucydides attributes to Hermocrates: "Nobody is driven into war by ignorance, and no one who thinks he will gain anything from it is deterred by fear . . . when there is mutual fear, men think twice before they make aggressions upon one another."

In the 1970s, behavioral scientists began to open new windows into the mind. The 2002 Nobel Prize in economics went to Princeton psychologist Daniel Kahneman for his work in the 1970s and 1980s on the psychology of judgment and decision making. Kahneman and his colleagues argued that people do not employ rational decision making in their actual processes in life; they do not try to collect all the possible information available to maximize the payoff of existing choices. Instead, they place boundaries on the kinds and types of data they collect and then employ "rules of thumb" rather than complex formulas of utility to rationalize choices. Such "bounded rationality," according to Kahneman, leads to errors of judgment from emotional bias and from using faulty decision-making heuristics.

Real-world case studies have shed new light into the psychology of national leaders when nuclear weapons might be involved in crises.[7] Many behavioral scientists have attempted to minimize the impact of such bias and develop methods to apply the ideal, rational decision-making model. In his famous book, *Every War Must End*, Fred Ikle wrote,

> It is not enough that those who can deliberately start a war should at no time come to believe that their nation, or their "cause," would be better served by going to war than if peace were maintained. For even if this condition is met, it will not be sufficient if wars can be started by . . . leaders who fail to think coherently about how the fighting will end, or who, in some perverse stubbornness, no longer care if it ends in disaster for their own country.[8]

The reality of the growing complexity of deterrence means that we have much to gain from deeper understanding of how to apply the behavioral approach to deterrence operations.

Emerging Domains of War—Cyber and Space

Cyber and space domains are contributing a tremendous measure of complexity to the challenge of deterring future adversaries. Deterrence and escalation control now cross multiple domains of war. Attacks against space assets intended to blind or dazzle for tactical or operational effect may be perceived as precursors to broader, deeper strategic attacks. Computer network attacks may have huge unintended consequences for the entire global system. And new conventional capabilities may have far-reaching deterrent effects. In Europe, for example, while the United States and Russia argue over the role of ballistic missile defenses in our strategic relationship, some assert that the alliance can afford to trade off nonstrategic nuclear capabilities while deploying ballistic missile defenses. Also, there is an emerging debate on the deterrent value of conventionally armed intercontinental missiles that could fly a ballistic trajectory for part of their path and then shift to a more maneuverable mode during reentry.[9] Such complex escalation and deterrence relationships heighten the potential for misperceptions and increase the risks of unleashing catalytic escalation forces.

In this milieu, Herman Kahn's ladder of escalation is less helpful as a mental model of deterrence. In a bipolar world, escalation was linear. Now, escalation can function across many dimensions not limited to the nuclear escalation ladder. In the multipolar, proliferated nuclear world, deterrence exists across at least four domains simultaneously—conventional, nuclear, cyber, and space. Dr. Chris Yeaw, Air Force Global Strike Command's chief scientist, likened this to a vortex in which each side could escalate or deescalate simultaneously across multiple domains and even jump from one ladder to another, making crisis management and escalation control much more complicated.

Ten Axioms for Campaign Planners

Today we must deter across multiple domains in local, regional, and global wars in a multipolar, proliferated nuclear world. While devoting the weight of effort to winning current fights and advancing the operational art of counterinsurgency and counterterrorism campaigns—and future complex hybrid operations—we cannot afford to neglect the important prospects of campaigns of the future that will carry greater risk and con-

sequence. To begin reinvesting our intellectual capital in deterrence, military professionals should consider several fresh approaches.

Go to School on Deterrence and Nuclear Doctrine

The 2010 *Joint Operating Environment* states the following: "For the past twenty years, Americans have largely ignored issues of deterrence and nuclear warfare. We no longer have that luxury."[10] Illustrative of the point is Air Force Doctrine Document (AFDD) 3-72, *Nuclear Operations*,[11] the only doctrinal manual in the US Department of Defense on the conduct of campaigns involving nuclear weapons. While it provides a solid grounding in the basics, it needs to be revised to account for the new US strategy and the Nuclear Posture Review. US STRATCOM's *Deterrence Operations Joint Operating Concept* provides a more expansive treatment but, as with all JOCs, it is aimed at guiding the development of future capabilities rather than the conduct of campaigns. Also, English translations of China's military doctrine on deterrence are available in open sources.[12] Campaign planners across the joint forces should read these documents. And, they should be taught in service schools.

Apply Deterrence in Each Phase of the Campaign

Joint Publication 3-0, *Joint Operations*, and the Joint Operational Planning and Execution System (JOPES) label Phase I of a joint campaign "Deter," and in practice joint forces also have implied tasks for deterrence across each phase; they may also have specified deterrence tasks in any phase.

Phase 0: Shape. Strategic shaping occurs every time the US Air Force and the Navy conduct test launches of ICBMs from Vandenberg AFB and from Trident ballistic missile submarines. Data sharing between the United States and Russia in accordance with arms control agreements also shapes the stability of our mutual deterrence relationship.

No matter what the particular mission assigned in any theater, the US military will be building partner relationships that contribute to its capacity to deter potential adversaries, reassure allies, and maintain the stability of the central nuclear balance among the United States, Russia, and China. When the last Tomahawk land attack missile–nuclear (TLAM–N) is retired from the Navy's arsenal, only dual-capable aircraft (nuclear-capable B-52 and B-2 bombers, F-16 and F-15 fighters, the F-35 Joint Strike Fighter, and NATO Tornado aircraft) will be available to provide visible evidence of our capability to conduct nuclear operations. These capabilities

send a message to key allies who rely on the US extended deterrence umbrella, allies who might otherwise feel compelled to seek their own nuclear capabilities. The continuous bomber presence mission in Pacific Command is a visible signal of US potential during real-world Phase 0 operations.

Phase I: Deter. In this phase, standard "flexible deterrence options" (FDO) are available to demonstrate US capability and resolve with the intent of causing the adversary to deescalate and avoid hostilities. The Joint Advanced Warfighting School of the Joint Forces Staff College teaches that FDOs are

> pre-planned . . . actions carefully tailored to send the right signal and influence an adversary's actions . . . developed for each instrument of national power—diplomatic, informational, military economic, and others (financial, intelligence and law enforcement DIMEFIL)—but they are most effective when used in combination with other instruments of national power . . . FDOs facilitate early strategic decision making, rapid de-escalation and crisis resolution by laying out a wide range of interrelated response paths . . . confront the adversary with unacceptable costs for its possible aggression.[13]

Examples of military FDOs include increased readiness posture, alert status, and force protection measures; heightened intelligence, surveillance, and reconnaissance; show-of-force actions; public diplomacy and strategic communications; and deployment orders that move military forces into the joint operations area without placing US forces in jeopardy if deterrence fails.

Typical post–Cold War FDOs eschew employment of nuclear capabilities, but the growing complexity of deterrence in a multipolar, proliferated nuclear world may require demonstrating the potential to employ the strongest military measures. Deployment of nuclear-capable airpower remains available to signal US capability and resolve visibly and flexibly. When the force structure implementation of the 2010 Nuclear Posture Review (NPR) is decided, there likely will be a number of nondeployed strategic nuclear delivery vehicles that will provide additional FDOs that may include movement of hedge warheads and stored ICBMs. The NPR also calls for development of "other basing modes" of ICBMs that may provide additional nuclear FDOs in coming decades. Space, cyber, and future conventional capabilities provide an even wider range of additional FDOs. Campaign planners need to be schooled in the full array of military capabilities available for FDOs.

Phase II: Seize the Initiative. For this phase of the joint campaign, future global strike capabilities will provide forces that can prevent an opponent from initiating combat on its terms. Conventional warheads contained in maneuverable, trans-atmospheric vehicles launched on ballistic missiles—systems that are not prohibited by arms control treaties—may enable limited, prompt global strikes that can deny an opponent the benefit it may seek from employment of its limited number of nuclear weapons. For example, a North Korean Taepodong ICBM on the launch pad with a nuclear warhead might be destroyed with a conventional munition within less than an hour of a launch order from the president. Theater campaign planners need to know how to employ and coordinate such strikes as deploying forces stage into the theater.

In some cases, it may be that conventional war-fighting capabilities are insufficient to seize the initiative. In those situations the joint force commander may choose to employ space or cyber capabilities to pave the way for an ensuing decisive operations phase. The capacity to conduct such operations would provide theater campaign planners with powerful deterrent threats. The theater joint force employed in cyber and space operations will also need to have robust, layered missile defenses as a means of deterrence by denying the enemy any benefit from ballistic missile strikes against US forces in the theater.

Phase III: Decisive Operations. The main effort of a joint campaign is to defeat the opposing force in Phase III. Generally this will be conducted by employment of decisive conventional combat power. But in dealing with a nuclear-armed opponent or nuclear-armed ally of a conventionally armed opponent, prudent joint campaign planners will need to prepare branches and sequels that anticipate potential first use of nuclear weapons by a risk-acceptant adversary. Here, again, the theater campaign planner may have future global strike capabilities available to support deterrence during the Phase III main effort. The Air Force chief of staff has said, "The future will call for at least as much if not more deterrence" capability than the service currently wields. Gen Norton A. Schwartz called for a low-cost, flexible family of systems that can meet many possible needs, from precision strikes in an asymmetric environment to full-scale bombing campaigns against heavily defended airspace, centered on a "penetrating bomber."[14] Future theater campaigns will have to incorporate such capabilities into Phase III planning.

Phase IV: Transition. Deterrence is not irrelevant to the ending of hostilities and termination of conflict. Capabilities that create fear of consequences in an opponent that has been defeated, is exhausted, or just wants to quit the fight remain important.

Consider the case of the Korean War. In 1950, after the Inchon landing enabled UN forces to fight their way back up the peninsula from the Pusan perimeter, Russia and China rejected any negotiations until all foreign troops were withdrawn. In 1951, after the advance into North Korea, General MacArthur was relieved. Then China dropped its demand and, with North Korea, agreed to a cease-fire along the demarcation line. But the fighting continued for two more years as North Korea and China insisted on mandatory repatriation of prisoners of war captured by UN forces and held in the south. Casualties mounted, reaching numbers greater than those before the cease-fire. In 1952 Dwight D. Eisenhower was elected US president and sought an end to the war by communicating nuclear threats to China and North Korea through third parties. He approved military planning to move atomic artillery and aerial bombs into place; operational staffs ordered their movement into position; commanders readied these nuclear forces for employment in a campaign to be executed on order if the enemy continued to be intransigent. Preparations for use of atomic weapons were made apparent to the Chinese and the North Koreans. When Joseph Stalin died in 1953, his successors put pressure on the Chinese and North Koreans to adopt a more conciliatory posture, and the communists finally accepted voluntary repatriation and a truce at Panmunjom.[15]

Phase V: Enable Civil Authority. Upon cessation of hostilities, military capabilities will still be important to provide deterrence of potential adversaries not involved in the fight who might nevertheless seek to achieve advantage presented by the opportunity of a neighbor's defeat or the disorder that could ensue from the lack of civil authority in a provisional military occupation. If the conflict involves nuclear weapons, US deterrence capabilities will be critical for providing an umbrella of protection while civil society is rebuilt.

Do No Harm to the Stability of Central Strategic Deterrence

The nuclear great powers will watch any crisis involving the United States very closely. Even if the strategic nuclear balance among the United States, Russia, and China becomes more stable, this will not guarantee continued stability in economic, political, or diplomatic competitions.

Regardless, in future conflicts we will continue to find ourselves risk-averse to provoking heightened concerns for the vital national interests of Russia and China. It will be particularly important to consider the implications military action against a particular adversary will have on its neighbors in this n-power game.

There is reason for special concern in this regard for the stability of our relationship with China, for we hardly know them. In the Cold War we devoted billions of dollars and enormous human resources in trying to learn how the Soviets made strategic decisions, to discern their intent, and to assess their true capabilities. And sometimes we still got it wrong. We have devoted nothing near that effort to understanding the intentions and capabilities of China.

It is equally important for them to understand us. At least Chinese strategists can study our Cold War crisis behavior. We can be sure that they read Schelling and Allison, but will that explain what our twenty-first-century redlines would be? How would the United States respond to a Chinese high-altitude detonation of an electromagnetic pulse weapon? Does the United States consider attacks in outer space to be akin to attacks on our soil? These kinds of questions go beyond our declaratory policy, reaching to the essence of our decisions. Not only are China's military writings more guarded and enigmatic than ours, they have never had a nuclear crisis of their own from which to learn about the pressures and stresses that affect communication of intent when a strategic nuclear exchange potentially hangs in the balance.

Maintaining crisis stability in a multipolar nuclear world requires more stringent assumptions about communication, trust, and commitment than with only two players, where weaker assumptions might suffice. Since the permutations and combinations inherent in multiactor crises are more numerous, creating confidence-building measures among nuclear-armed states may become a particularly useful method for building crisis stability. Military-to-military exchanges cannot guarantee friendliness, but they can promote understanding.

Such exchanges could produce deeper understanding of the strategic cultures of nations and nonstate groups that might acquire nuclear weapons. Culture plays a large role in strategic relationships; therefore, it will serve us well to invest in the kind of cultural understanding only prolonged effort provides. During the Cold War, the United States and the Soviet Union both reflected the world of the enlightenment in advancing their own

unique "internationalisms"—democracy in the case of the United States, communism for the Soviet Union—according to Prof. Paul Bracken, who notes,

> Compare such noble internationalisms with nationalism driving the new nuclear states. Pakistan uses Islamic fundamentalism to try to build an extension of nationalism in Afghanistan and Central Asia; North Korea seals itself off from the outside world with a *juche* philosophy of self-reliance and convinces its people that they are respected by the countries of Asia. These behaviors arise out of an emotional nationalism that one people is better than another. The United States and the Soviet Union had their own absurd ideas, to be sure. But neither believed that their peoples were innately superior to each other, only that their core political beliefs were.[16]

Understand the Limits of Conventional Deterrence

There have been many debates in the United States on the value of conventional deterrence. Indeed, the Nuclear Posture Review sets us on a path to zero nuclear weapons in part based on the belief that conventional means may one day fully substitute for nuclear weapons. Surely our 4,000 years of human history with conventional warfare—compared to 65 or so with nuclear weapons—can teach us something empirically about the efficacy of conventional deterrence.

In the 1980s Paul Huth and Bruce Russett conducted an interesting statistical study of deterrence.[17] They looked at 54 case studies of twentieth-century warfare in which one side attempted an initial deterrence strategy and then applied a methodology to normalize all the appropriate factors so they could draw comparisons among the studies. They concluded that, historically, deterrence has worked a little more than half the time (31 out of 54 cases) and nearly always by denial of benefit rather than by imposing cost. They also found that it never worked in great-power wars, only in regional conflicts. And, when deterrence did work, there was usually both a strong relationship between a great-power defender and its protégé as well as a record of arms transfers from the defender to its protégé. In the six instances in which at least one side was a nuclear power, possession of nuclear weapons by the defender had no effect on the success or failure of deterrence in preventing the outbreak of war.

Conventional deterrence, then, might work about half the time. Campaign planners who must develop flexible deterrent operations should study Barry Blechman's comprehensive analysis from the 1970s of what

worked and what did not when conventional forces were employed to affect the decision-making processes of potential adversaries.[18] This was an exhaustive analysis of dozens of Cold War–era case studies and is well worth rediscovery for the twenty-first century.

Plan for Operations on a Nuclear Battlefield

If it is now much more likely that some rogue state or nonstate actor will detonate a nuclear weapon in our lifetime, or if the consequence of a multipolar nuclear world is greater risk of nuclear war through miscalculation, then it stands to reason that we must prepare our forces for operations on a nuclear battlefield, even if we do not resort to first use or responding in kind ourselves. There is growing concern in the analytic community about the prospects for limited nuclear war in the near future.[19] Even novelists are speculating on how radical Islamist organizations possessing a number of nuclear weapons might use them in an operational campaign as opposed to the usual scenario of detonating a single device in a major Western city during a terrorist attack.[20]

We are ill prepared for this. While there are regulations, procedures, and joint doctrine for managing the consequences of an adversary's use of weapons of mass destruction, there is no doctrine for conducting combat operations on a nuclear battlefield.

Assess the Credibility of Deterrence

How do you judge a negative? That is, how do you know your attempts at deterrence are successful? What indicators and warnings reveal the enemy's intent? What are the priority intelligence requirements for a deterrence campaign or line of operation? Is the opponent not attacking because it is deterred or because it is just biding its time for a massive response that you did not anticipate? There are many who argue that answers to these questions are simply unknowable and deterrence must rest on blind faith, or that the planner will have to conduct operations as if the deterrence phase will fail—a stratagem that, of course, risks self-fulfillment.

Some recent methodological and empirical work can help campaign planners discern whether deterrent threats are achieving the intended effects of creating fear of consequences in the opponent's calculations. Daryl Press conducted case studies into instances of a country communicating deterrent threats to an opponent to prevent the outbreak of war among great powers. He looked at German assessments of British and French

threats in 1938–39, British and US assessments of Soviet threats in the Berlin crises of 1958–61, and US assessments of Soviet threats in the Cuban missile crisis of 1962. Press found that deterrence works when a country makes threats that the opponent believes it is capable of carrying out and when the opponent believes its adversary has a strategic interest in doing so. In other words, the prerequisite for deterrence has less to do with rational calculations of risk and intent, even if the adversary has a reputation for bluff, bluster, and subterfuge. The success or failure of deterrence in those cases had more to do with perceptions of capability and willingness; what matters most is the here and now, not past behavior.

This suggests that assessing the credibility of a deterrent threat should begin with an objective look at what the Soviets called "correlation of forces," or the military balance that can be brought to bear in a crisis. We discovered with the Soviets that different sides can have different ways of measuring military power, so it will be prudent to maintain a capacity to emulate the potential adversary's military analysis and decision-making processes to reflect accurately its understanding of our military capability. It may use measures of merit quite different than our own and combine them in ways that would appear strange to our own method of conducting campaign analysis. In any case it is vital not to fall prey to the temptation of mirror imaging when conducting an assessment of the credibility of a deterrent threat.

Press also suggests several ways to assess intent. He asserts that "[t]he evidence for credibility is in the adversary's private communications about their perceptions of our capabilities and intentions and their reasoning behind their own policies."[21] In his four case studies, Press found strong support for the conclusion that there are two primary sources of evidence about the credibility of a deterrent threat in the mind of the adversary. First, we can turn to the opposing decision makers' statements about their adversary's credibility. They often make statements about their expectation of the explicit likelihood that we will carry out our threats and promises. Second, Press says to look at the very policies that decision makers advocate during crisis. Credible threats generate more calls for concessions than do threats that are not credible. If the opponent decision makers advocate a hard-line policy, they do not believe our threat is credible. If they argue for caution, they assign higher credibility to our threat.

Press' historical case studies rely on archival source material for a retrospective look at what deterred and what did not. Campaign planners will,

of course, not have the luxury of hindsight or even foresight to see into the enemy's decision making in the future. However, today's information operations tools can provide timely insights into the kinds of evidence that are needed to assess credibility of deterrent threats. We should be particularly capable of developing communications intercept and computer network exploitation that would allow collection of timely intelligence on the opponent's internal communications. A number of tools exist for exploiting massive amounts of data to discern relevant content that would reveal the kinds of discussions Press suggests would shed light on the credibility of our deterrent threats in the minds of our opponents. Campaign planners need access to those kinds of intelligence capabilities and analytic tools.

Beware the Potential for Cascading Effects

If escalation is more like a vortex than a ladder, then chances are a crisis in the multipolar, proliferated nuclear world will be more like 1914 than 1939 in terms of its potential for spiraling out of control. The twenty-first century is fraught with risks of misperceptions among crisis participants from divergent cultural perspectives and with clashing strategic interests. These risks are compounded by the fact that every newly nuclear state goes through a period of learning about its new role; it must learn both how it intends to employ its nuclear capabilities to achieve their deterrent effects and how to keep them safe, secure, and reliable in their particular geopolitical environment. Unanticipated consequences abound with emerging warfare domains such as cyber and space. Timelines for decision, already made very short by the Cold War capabilities of ballistic missiles, will be even further compressed by nearly instantaneous and ubiquitous effects of a globally interconnected world order.

In this milieu, decision superiority will become a capability of military necessity. Decision superiority is simply the capacity to make better decisions faster than opponents. Sometimes this will depend on one's own command of the "observe, orient, decide, act" cycle. But in many exercises, experiments, and war games, the military has discovered that it just cannot execute the "orient" phase fast enough to get inside some opponents' decision cycles. This is particularly evident in exploring how to conduct ballistic and cruise missile defense against a sophisticated opponent who employs not only very capable missiles but also large numbers of them in complex operational concepts of attack (e.g., surge, swarm,

multiple, and changing directions). There is an emerging concept for command and control that suggests we will need military capabilities to enable us to decide and begin to act well before we have traditionally sufficient information to conduct the military decision-making process. Another complementary approach for achieving decision superiority may lie in the conduct of denial, deception, and disruption concepts to slow down and degrade the opponent's decision cycle.

We can develop ways to make decisions faster, but will they be good decisions? How do we provide decision-making support that enables not only *faster* decisions but also *better* decisions? In carrying out twenty-first-century deterrence operations, we need to make decisions that are better in the sense that they produce actions that not only achieve our geopolitical objectives but also do not trigger a chain of consequences that result in nuclear weapons use. Here again, we need more work in the behavioral model of decision making rather than the rational actor model.

Leverage the Cognitive Domain of War

When he served as director, force transformation in the office of the secretary of defense, RADM Art Cebrowski asserted that wars are won or lost in the cognitive, rather than in the physical, domain.[22] By this he meant that the information revolution has ushered in a new era in which mastery of the physical domain of war is no longer sufficient. His thinking on this is most applicable to the problem of deterrence in the twenty-first century, where we must develop military campaigns to deter the use of nuclear weapons by a variety of potential adversaries.

Kahneman's behavioral science approach to economics is built on Herbert Simon's pioneering work on prospect theory of choice making, describing how decisions are made among alternatives with uncertain risks. Kahneman extended prospect theory to examine more closely the biases and heuristics in human decision making.[23] The prospect theory school of decision making asserts that, although such skewed thinking was generally successful, or at least good enough for economic satisfaction if not maximization of utility, nevertheless the impact of such bias could be minimized to approach the ideal, rational decision-making model.

In the 1990s an alternative behavioral school emerged in contrast to Kahneman's adaptation of prospect theory, suggesting that such heuristic decisions are after all quite natural and, in terms of efficiency in doing the things necessary for human progress—namely survival, evolution, and

domination by the species—often even better than optimizing strategies. What Kahneman found to be bias, deflecting the human mind from the ideal, researchers such as Gary Klein and Gerd Gigerenzer viewed as adaptive, emergent behavior. Their field research suggests that humans, perhaps regardless of culture, make decisions based on a few common heuristics that enable decision making that is fast enough to avoid falling prey to other species and sufficiently frugal in terms of exploiting the cognitive capacity of the human brain to seek and absorb only enough information necessary to make the decisions at hand.

Klein conducted over 600 field studies of experienced, successful decision makers who were confronted with situations involving incomplete information, uncertainty, high risk, and intense time pressures (e.g., fire fighters, tactical and operational military staffs, medical professionals, nuclear power plant operators, etc.). He concludes, "The evidence that supposedly shows that stress results in decision errors is not convincing . . . experienced decision makers adapt to time pressures very well by focusing on the most relevant cues and ignoring others."[24] Klein argues there are some common sources of error that might be useful for campaign planners to understand and train to minimize. For example, *de minimus sorting* occurs when people in the decision-making chain are aware of disconfirming evidence and may even seek it out but then explain it away; Klein and his research team dissected the USS *Vincennes'* shoot-down of the Iranian airliner in 1988 and concluded that this was the root cause of that error.

Confirmation bias occurs when a person chooses to seek confirming evidence that has little diagnostic value because it cannot help distinguish between alternative hypotheses and does not try to obtain other diagnostic evidence that might disconfirm the favored hypothesis. He cites the example of the 1973 shoot-down of an off-course Libyan civilian airliner by the Israelis as a case of this type of error.

Klein posits that training on countermeasures to such errors would prove useful to campaign planning staffs. One such technique he calls *pre-mortem mental simulation*—a technique especially useful for planners who are often overconfident about the plan they created. This technique asks planners to imagine their plan was executed and failed. The pre-mortem helps reveal hidden or understated risks.

Gigerenzer has focused on laboratory and field research aimed at understanding the elements of the cognitive domain. He suggests that all human decision making boils down to three components that form a heuristic:

search rules used to limit the volume of data considered, *stopping rules* to limit the amount of time and effort spent on collecting data, and *decision rules* to apply in making choices among alternatives.

> Humans and animals make inferences about their world with limited time, knowledge, and computational power. In contrast, many models of rational inference view the mind as if it were a supernatural being possessing demonic powers of reason, boundless knowledge, and all of eternity with which to make decisions . . . we propose replacing the image of an omniscient mind computing intricate probabilities and utilities with that of a bounded mind reaching into an adaptive toolbox filled with fast and frugal heuristics.[25]

If this is so, then military decision making across cultures and across the ages may be reducible to a shared set of common fast and frugal heuristics. If we could determine what some common military decision-making heuristics are, then maybe we could better anticipate an opponent's decision as it is made, perhaps even in advance.

Do Not Assume Opponents without Fear Cannot Be Deterred

Too many military planners assert that defiant proliferators and terrorists are irrational and cannot be deterred, so the only option is that they be killed or captured. There is no empirical analysis to support that argument. There is indeed evidence that rogues and nonstate actors who possess weapons of mass destruction and their means of delivery can be deterred.

Deterrence worked in 1991. The United States conveyed the not-so-veiled threat that if the Iraqis used chemical or biological weapons on US troops, then we would respond with nuclear weapons. Although Tariq Aziz said later that he did not take President Bush's letter to Saddam, we now know that the message was indeed conveyed and that Iraqi generals took it seriously.[26] Indeed, there is emerging evidence that Saddam himself was convinced that the United States would use nuclear weapons on Iraq if he were to order or authorize use of chemical weapons on American troops in the 1991 Persian Gulf War.

Rather than assuming terrorists cannot be deterred, we should conduct the necessary behavioral research to determine just where their fears lie, then apply the threat of military power to create the desired effects on their behavior. Since 9/11 Dr. Jerrold Post, a long-time consultant to the CIA, has studied all major terrorist groups and is one of only a few who has interviewed hundreds of detainees from the war on terror. Dr. Post reports on his interviews,

> [T]wo responses from the terrorists deserve emphasis . . . one concerned the fear of these weapons, of "the silent death," of infectious microbes, deadly toxins and radioactivity. Not everyone wishes to be a martyr, and the danger of handling these deadly chemical, biological, and radiological materials should be emphasized. The second theme was the proscription in the Koran against mass casualties, including killing innocents, and the requirement to not poison the earth and living things.[27]

We need to identify such fears and how nuclear weapons can threaten in ways that speak to those fears.

Develop Innovative Tactical and Operational Forms

Finally, lacking a playbook, we need to develop ways to apply deterrence in this multipolar, proliferated nuclear world. In my own experience across a number of war games and exercises, it is clear that the process of developing deterrence courses of action has become a lost art. Few players or staffs have a sense of the range of capabilities available for deterrence operations, and fewer still have a nuanced understanding of what might deter the particular adversary. In such events, most participants arrive with the deterrence belief that "one size fits all" situations but then quickly come to realize that nuclear deterrence is not a pickup game.

A number of analysts have suggested we need more accurate nuclear weapons with low-yield options to make deterrence credible at the operational level. They argue this would be the case for both regional adversaries and peers.[28] They believe it would work by enabling US forces to hold sanctuaries at risk while minimizing collateral damage to levels even lower than those that would occur if conventional weapons were used.[29] If this approach were adopted, it would require that joint force campaign planners experience a rebirth of expertise in nuclear operations.

New forms of deterrence operations can be developed for this multipolar, proliferated era in which deterrence has grown increasingly complex. We must resurrect joint doctrine for nuclear operations and revise Air Force nuclear operations doctrine. Additionally, the art of military campaign planning must incorporate techniques and procedures for deterrence operations, including deterrence lines of operations that provide deterrence branches and sequels extending across all phases of the joint force campaign. We must involve expert, live, red teams that will produce insight into opponent military decision-making processes while fielding a new generation of analytic tools for planning staffs to measure and assess the credibility of their deterrence planning efforts.

Deterrence Across the Ages

There are those who assert that deterrence is greatly overrated, poorly understood, and desired today mostly out of nostalgia. Not so. Campaign planners in operational joint forces around the globe increasingly find themselves confronted with the challenge of developing concepts of operations that will in practice provide commanders with a realistic likelihood of deterring potential adversaries who are willing to take on the United States of America. The growing complexity of deterrence compels military professionals to develop ways to plan and achieve deterrence at the operational level of war.

Deterrence is a World Cup sport, and we are only beginning to reinvigorate our state of conditioning to play the twenty-first-century game. The practice of deterrence has fundamentally changed, and all the thinking and theorizing we might do should be translated into capabilities and playbooks for the real world. As the United States continues to strengthen its nuclear enterprise, we need to advance the art of deterrence campaign planning and toughen our practices. Deterrence at the operational level of war is an idea whose time has come. SSQ

Notes

1. See http://www.STRATCOM.mil.
2. "While the most important mission of the American military has been to fight and win the nation's wars, the ability of U.S. forces to deter conflict has risen to equal footing. Preventing war will prove as important as winning a war." US Joint Forces Command, *The 2010 Joint Operating Environment*, 18 February 2010, 60.
3. US STRATCOM, *Deterrence Operations Joint Operating Concept*, ver. 2 (Washington: Office of the Secretary of Defense, December 2006), 8.
4. "Proliferation Status 2009," http://www.carnegieendowment.org/files/2009-global-prolif6.pdf.
5. Andrew J. Coe and Victor A. Utgoff, *Understanding Conflicts in a More Proliferated World* (Institute for Defense Analyses, Report P-4426, December 2008).
6. James Fallows, *National Defense* (New York: Random House, 1981).
7. Robert Jervis, Ned Lebow, and Janice Stein, *Psychology and Deterrence: Perspectives on Security* (Baltimore: Johns Hopkins University Press, 1989).
8. Fred Charles Ikle, *Every War Must End*, 2nd ed. (New York: Columbia University Press, 2005).
9. Bruce Sugden, "Speed Kills: Analyzing the Deployment of Conventional Ballistic Missiles," *International Security* 34, no.1 (Summer 2009): 113–46.
10. *Joint Operating Environment* (Suffolk, VA: US Joint Forces Command, February 2010), 53.
11. When published on 1 June 2009, *Nuclear Operations* was designated Air Force Doctrine Document 2-12. The Air Force has since restructured its doctrinal publications, and *Nuclear Operations* is now AFDD 3-72.

12. See footnote 4 in Mark A. Stokes, *China's Nuclear Warhead Storage and Handling System*, 12 March 2010, Project 2049 Institute, http://project2049.net/documents/chinas_nuclear_warhead_storage_and_handling_system.pdf.

13. *Operational Art and Campaigning Primer AY 09-10: Joint Operation Planning Process* (Washington: Joint Advanced Warfighting School, 2009), 334, http://www.jfsc.ndu.edu/schools_programs/jaws/Campaign_Planning_Primer_2010v-4.pdf.

14. John Reed, "Schwartz: Air Force needs new long-range bomber," *Air Force Times*, 14 September 2010, http://www.airforcetimes.com/news/2010/09/defense-schwartz-air-force-new-bomber-091410/.

15. For more detail, see Max Hastings, *The Korean War* (New York: Simon and Schuster, 1987), 318–20. For an analysis as a case study in compellance and deterrence, see Alexander L. George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 235–41. For a revisionist interpretation, see Rosemary J. Foot, "Nuclear Coercion and the Ending of the Korean Conflict," *International Security* 13, no. 3 (Winter 1988–89): 92–112.

16. Paul Bracken, "The Structure of the Second Nuclear Age," Foreign Policy Research Institute, 25 September 2003, http://web.mit.edu/ssp/seminars/wed_archives_03fall/bracken.htm.

17. Paul Huth and Bruce Russett, "What Makes Deterrence Work? Case Studies from 1900 to 1980," *World Politics* 36, no. 4 (July 1984): 496–526.

18. Barry M. Blechman and Stephen S. Kaplan, *Force without War: U.S. Armed Forces as a Political Instrument* (Washington: Brookings Institution, 1978).

19. *Limited Nuclear War* (Washington: Institute for National Strategic Studies, forthcoming 2011).

20. Ralph Peters, *The War after Armageddon* (New York: Tom Doherty Associates, 2009).

21. Daryl G. Press, *Calculating Credibility: How Leaders Assess Military Threats* (Ithaca, NY: Cornell University Press, 2005).

22. James Blaker, "Arthur K. Cebrowski: A Retrospective," *Naval War College Review* 59, no. 2 (Spring 2006): 129–45.

23. Daniel Kahneman biography, http://nobelprize.org/nobel_prizes/economics/laureates/2002/kahneman.html.

24. Gary Klein, *The Sources of Power: How People Make Decisions* (Boston: MIT Press, 1998).

25. Gerd Gigerenzer, Peter M. Todd, and the ABC Research Group, *Simple Heuristics That Make Us Smart* (New York: Oxford University Press, 1999).

26. Keith B. Payne, "On Nuclear Deterrence and Assurance," *Strategic Studies Quarterly* 3, no. 1 (Spring 2009): 43–80.

27. Jerrold Post, *The Mind of the Terrorist* (New York: Palgrave MacMillan, 2007).

28. See Jason Zaborski, "Deterring a Nuclear Iran," *Washington Quarterly* 28, no. 3 (Summer 2005): 153–67, regarding credibility vis-à-vis adversaries and Keir Lieber and Daryl Press, "The Nukes We Need," *Foreign Policy* 88, no. 6 (November/December 2009): 39–51, in the case of peers.

29. Payne, "On Nuclear Deterrence and Assurance."

Considerations for a US Nuclear Force Structure below a 1,000-Warhead Limit

David J. Baylor, Colonel, USAF

On 5 April 2009 in Prague, Czech Republic, President Obama committed the United States to seeking "the peace and security of a world without nuclear weapons."[1] This move toward a nuclear-free world is not a new idea. In January 2008, George P. Shultz, William J. Perry, Henry Kissinger, and Sam Nunn authored an article for the *Wall Street Journal* suggesting steps to "dramatically reduce nuclear dangers." More than a dozen former senior US officials from the past six administrations endorsed these suggestions.[2] While these officials offered "suggestions," they realized the challenge of achieving a nuclear-free world would be difficult. In fact, the president recognized this challenge in his Prague speech when he stated, "This goal will not be reached quickly—perhaps not in my lifetime." "Just as importantly," the president added, "As long as these weapons exist, the United States will maintain a safe, secure and effective arsenal to deter any adversary, and guarantee the defense of our allies."[3] In a move toward a nuclear-free world, Obama and Russian president Medvedev signed the "New Strategic Arms Reduction Treaty (START)" on 8 April 2010 in Prague, limiting deployed strategic warheads to 1,550. This is a 30-percent reduction from the 2002 Moscow Treaty, moving the world one step closer to eliminating all nuclear weapons.[4]

As the president moves toward a nuclear-free world, we must ask some very important questions about that journey: (1) Do different negotiation considerations and dynamics come into play when Russia and the United States go below 1,000 strategic warheads? (2) What are the implications of nonstrategic or tactical nuclear weapons in the global security environment? and finally, (3) What are the potential implications for the US nuclear

---

Col David "DJ" Baylor is a master navigator with more than 2,000 hours in F-111s and B-1 bombers. He holds a BS degree in mechanical engineering from the Pennsylvania State University; a master of aeronautical science, Embry-Riddle Aeronautical University; a master of military operational art and science, Air Command and Staff College; and a master of strategic studies from the Air War College, Maxwell AFB, where he included an emphasis in nuclear threats and countermeasures through the USAF Counterproliferation Center and a regional and cultural study on Northeast Europe and Russia.

force structure and the impact on the role of nuclear deterrence as its national arsenal moves below 1,000 strategic warheads? These questions require a thorough analysis and invite "suggestions" on how the United States should proceed.

New Negotiation Dynamics below 1,000 Warheads

A world free of nuclear weapons is a noble goal and a commitment we have as a nation in accordance with Article VI of the Nuclear Non-Proliferation Treaty (NPT) as ratified by the United States in March 1970.[5] Over the past 40 years, the United States has negotiated directly with the Soviets, and now the Russians, to reduce our nuclear arsenals. While negotiations were difficult, viewed from a distance these talks were very similar to Newton's Third Law of Motion: "For every action there is an equal and opposite reaction."[6] This is not to say there was a one-for-one reduction in warheads between the two nations. But as one nation proposed an action to reduce weapons, the other responded with what it saw as an equal reduction while always maintaining the status quo balance of power. As we move into a period where the United States and Russian arsenals are perhaps reduced below 1,000 warheads, we leave Newtonian physics of equal and opposite reactions and enter a new quantum physics world of negotiations where additional actors affect strategic and crisis stability with implications we do not yet completely comprehend.[7]

In this quantum physics view of nuclear arms reduction, we must look at numerous additional actors and forces—great and small—that will play important roles. These actors include current nuclear weapons states, aspiring nuclear weapons countries, other states with some nuclear technology, and US allies operating under the cover of its "nuclear umbrella."[8] To understand the impact that these countries will have on the negotiation process as we move toward a world free of nuclear weapons, we must first have a general understanding of their current positions in the world security environment and the directions they are moving. While it is impossible to know everything about each of these nations or their complexity, we will look at some important factors to consider as the United States and Russia move toward nuclear arsenals below 1,000 warheads and fewer associated strategic delivery vehicles.

To examine the players in a new world of ever-deeper cuts, we first look at those countries currently possessing nuclear weapons. Only five recognized

nuclear weapons nations have signed and ratified the NPT: the United States, Russia, China, France, and Great Britain. With its large nuclear arsenal, Russia possesses the greatest potential threat to US national security.[9] It is therefore against the Russian threat that US deterrent forces must be capably and properly sized. Likewise, the Russian government is no doubt concerned with deterring what it may perceive as a US threat to its existence.

With this mutual threat in mind, the presidents of the two countries have negotiated and signed the New Strategic Arms Reduction Treaty that the US Senate ratified with amendments on 22 December 2010 by a bipartisan vote of 71 to 26.[10] In response to the US midterm elections, the Russian parliament withdrew its recommendations for ratification, putting the future of the treaty in limbo.[11] While President Medvedev spoke positively about the US Senate ratification, he believed it "could take some time for the Russian lawmakers to study the amendments to the treaty."[12] At issue were two amendments added by the US Senate, one calling for modernization of the US nuclear triad and the other for discussion between the two counties on tactical nuclear weapons.[13] By 26 January 2011 both the Russian State Duma and Federation Council ratified the treaty adding their own amendments which include a provision for Russian withdrawal if the "US upsets the strategic balance with any major missile defense initiative."[14] The exchange of ratified and signed documents by Secretary of State Clinton and Russian foreign minister Lavrov on 5 February 2011 put the new treaty into effect.[15] The new treaty ends the hiatus of verification and inspection protocols that existed under the original START, which expired on 5 December 2009.[16]

The agreed upon New START limits are "(a) 700, for deployed ICBMs, deployed SLBMs, and deployed heavy bombers; (b) 1550, for warheads on deployed ICBMs, warheads on deployed SLBMs, and nuclear warheads counted for deployed heavy bombers; (c) 800, for deployed and non-deployed ICBM launchers, deployed and non-deployed SLBM launchers, and deployed and non-deployed heavy bombers."[17] This treaty will put the two countries on course to reach the lowest number of strategic nuclear weapons and delivery vehicles since the early 1950s for the United States and 1960s for Russia (see table 1), bringing both arsenals much closer in number to China and other nuclear-armed nations.

While publicly committing to a world free of nuclear weapons, Russia continues to replace its strategic nuclear warheads with new designs and delivery systems.[18] In recent defense budgets, it has allocated resources to

Table 1. Global Nuclear Weapons Inventories, 1945–2010

YEAR	UNITED STATES	RUSSIA	UNITED KINGDOM	FRANCE	CHINA	ISRAEL	INDIA	PAKISTAN	TOTAL
1945–1967									
1945	2								2
1946	9								9
1947	13								13
1948	50								50
1949	170	1							171
1950	299	5							304
1951	438	25							463
1952	841	50							891
1953	1,169	120	1						1,290
1954	1,703	150	7						1,860
1955	2,422	200	14						2,636
1956	3,692	426	21						4,139
1957	5,543	660	28						6,231
1958	7,345	869	31						8,245
1959	12,298	1,060	35						13,393
1960	18,638	1,605	42						20,285
1961	22,229	2,471	70						24,770
1962	25,540	3,322	288						29,150
1963	28,133	4,238	394						32,765
1964	29,463	5,221	436	4	1				35,125
1965	31,139	6,129	436	32	5				37,741
1966	31,175	7,089	380	36	20				38,700
1967	31,255	8,339	380	36	25	2			40,037
1998–2010									
1998	10,732	22,500	281	450	232	68	2	3	34,268
1999	10,685	22,000	281	450	232	70	8	8	33,734
2000	10,577	21,500	281	470	232	72	14	13	33,159
2001	10,526	21,000	281	350	235	74	20	18	32,504
2002	10,457	20,000	281	350	235	76	26	23	31,448
2003	10,027	19,000	281	350	235	78	32	28	30,031
2004	8,570	18,000	281	350	235	80	38	33	27,587
2005	8,360	17,000	281	350	235	80	44	38	26,388
2006	7,853	16,000	281	350	235	80	50	43	24,892
2007	5,709	15,000	225	350	235	80	60	50	21,709
2008	5,273	14,000	225	300	235	80	70	60	20,243
2009	5,113	13,000	225	300	240	80	80	70	19,108
2010	5,000*	12,000	225	300	240	80	80	70	17,995*

***The US column only includes warheads in the DoD stockpile, which was declassified in May 2010. Several thousand additional retired but intact warheads are awaiting dismantlement, probably 3,500–4,500 as of August 2010. (Adapted from R. D. Norris and H. M. Kristensen, "Global nuclear weapons inventories, 1945–2010," *Bulletin of the Atomic Scientists* 66 [2010]: 81–82).**

procure new dual-capable strategic bombers while also attempting to reinvigorate its fleet of nuclear submarines.[19] In addition, it is building new land-based RS-12M1/2 Topol-M intercontinental ballistic missiles (ICBM) with a multiple reentry vehicle (MIRV) capability.[20] Most importantly, Russia is placing more emphasis on its large stockpile of tactical nuclear weapons in its national defense strategy.[21] Its shift to a "first use" strategy is a counterbalance and cost-savings move while it downsizes and modernizes its conventional military forces.[22] With this increased reliance on nuclear weapons in a first-use capacity, it will be difficult for the Russians to reduce their nuclear arsenal below New START levels until they feel their conventional forces are equal or greater in capability to North Atlantic Treaty Organization (NATO) and Chinese nuclear and conventional forces on their borders.

While Russia poses the greatest existential threat to the United States, the next greatest threat comes from China. According to open sources, China possesses approximately 240 nuclear warheads, with perhaps 186 operationally ready for employment on aircraft or ballistic missiles. With such a small force, China appears to have adopted a minimum deterrence strategy. It has approximately 20 CSS-4 ICBMs able to reach the United States. The remaining warheads are programmed to be delivered by aircraft or short- and medium-range missiles.[23] The Chinese have publicly declared a "no first use" policy, with a self-defense nuclear strategy.[24] China defends against attack by developing underground facilities to house its nuclear weapons, providing for maximum survival of its arsenal from a first strike and guaranteeing a robust retaliatory capability.[25] Maintaining a secure second-strike retaliatory force rather than an insecure and vulnerable nuclear force is also more conducive to crisis stability.[26]

When we include the Chinese at the arms control negotiation table, we must consider their strategic situation, surrounded by nuclear-armed countries such as Russia, India, North Korea, and Pakistan and within striking distance of Iran and the United States. While China has formidable conventional forces, as long as surrounding countries have nuclear weapons the Chinese are unlikely to reduce their nuclear arsenal. Indeed, all countries with nuclear arms need to be included in future nuclear arms control treaty negotiations, including the United Kingdom and France.

The UK currently maintains approximately 160 nuclear warheads configured to be delivered only by submarine-launched ballistic missiles (SLBM) from four *Vanguard*-class Trident fleet ballistic missile submarines

(SSBN),[27] Researchers at the Stockholm International Peace Research Institute (SIPRI) believe that some UK missiles only contain one warhead and are configured for a "low yield" using only the "fission primary." The UK Ministry of Defense believes this "provides a 'sub-strategic' role to the Trident Fleet."[28] Britain has reduced its reliance on nuclear weapons since the end of the Cold War, and, from comments made by former Prime Minister Gordon Brown, it appears it is willing to reduce its purchase of new nuclear submarines by 25 percent, from four to three.[29]

France, on the other hand, possesses approximately 300 nuclear weapons widely dispersed on four SSBNs and 84 tactical aircraft.[30] Even though the French have recently rejoined NATO's Integrated Military Command after 43 years, they still pride themselves on a nuclear capability that could be used independently of the NATO command structure.[31]

While the UK, France, Russia, and China are all important nuclear powers and permanent members of the United Nations (UN) Security Council, when the United States goes below 1,000 strategic nuclear warheads, other nuclear weapons states will equally deserve a seat at the negotiating table. These additional countries—India, Pakistan, North Korea, and Israel—are not signatories to the NPT but already have, or in the case of Israel are believed to have, nuclear weapons.

India currently maintains an arsenal estimated at 60–70 tactical nuclear weapons delivered by aircraft along with short- and medium-range missiles.[32] India and its nuclear-armed rival Pakistan have fought three wars and continue to threaten each other, suggesting these two states must, at some point in the near future, be included in multilateral nonproliferation and nuclear arms control talks.

Pakistan is estimated to possess 60 tactical nuclear weapons delivered by missiles, along with enough plutonium and highly enriched uranium to produce 40 more.[33] It sees India's larger and technologically more advanced conventional military as an existential threat and will not give up its nuclear weapons, seen as equalizers, as long as this threat exists.[34] Pakistani leaders and citizens also enjoy the prestige conferred by their status as the only Muslim nation with nuclear weapons. While India and Pakistan should be essential players in future negotiations, we must also consider crafting agreements to take into account and limit states, such as North Korea, Iran, and Israel, that have or are pursuing nuclear weapons.

North Korea has twice demonstrated the ability to detonate a nuclear weapon while it refines its ICBM capabilities. Iran, already with a proven

short- and medium-range missile capability, continues to defy UN mandates as it develops its uranium enrichment technologies. Israel has chosen a nondeclaratory policy toward nuclear weapons, but some analysts estimate that it maintains approximately 100 nuclear warheads.[35] These three states, with their nuclear ambitions, influence and threaten the security of countries around them that either already have some nuclear technology or have the funding to acquire nuclear technology and weapons.

North Korea's nuclear ambitions, for example, affect the Republic of Korea and Japan. These are two of 30-plus countries under the US nuclear umbrella.[36] Japan has the technological knowledge to build nuclear weapons if it chooses.[37] In the Middle East, Iran's drive to acquire nuclear weapons has inspired other Middle Eastern countries, such as Saudi Arabia, Egypt, and Turkey, to consider pursuing enrichment capabilities.[38]

Prestige is an important consideration in future nuclear negotiations. Many countries, including the UK, France, India, Pakistan, Iran, and North Korea, see nuclear weapons not only as part of their national security policy but also as important status symbols, providing them influence in the international community and a seat at the table with the United States, Russia, and China. Asking these countries to give up their nuclear weapons and perceived political status in international relations will complicate all future nuclear arms negotiations directed toward that end.

Ironically, democracy will add one of the biggest unknown variables to all future negotiations. With elections held at periodic intervals throughout the various democratic countries around the world, internal politics of the moment can almost instantly change the direction a country takes regarding nuclear weapons, for example, the change of direction between the Bush and Obama administrations. The various NATO allies can easily change their stance on nuclear weapons and forward deployment of US nuclear weapons within their borders. The recent Japanese election demonstrates how an administration can take a significantly different approach, as demonstrated by its recently launched probe into reported "secret nuclear pacts" with the United States.[39] While all regimes, democratic or autocratic, can change their nuclear ambitions based on an opponent taking power, this is more likely to occur within democracies.

Another potential problem is that verification of compliance by 9–10 different nuclear-armed countries will slow progress and complicate nuclear disarmament talks. Current bilateral US and Russian negotiations have yielded an accepted inspection protocol that works in the current environ-

ment. However, future multinational negotiations may present numerous new questions:

- Can 10 different states agree upon a rigorous and adequate verification regime?
- What kind of international inspectorate can be formed?
- Will each state be willing to open its territory to adequate types of inspections?
- What role will the UN play in treaty execution?
- How does the United States manage and verify stockpiles to ensure other nuclear states do not reweaponize?
- How do we prevent countries from breaking their treaty obligations, thereby gaining strategic advantages denied to others?
- As we disarm further, can we ensure protection for allies currently under the US nuclear umbrella?
- Will these countries pursue their own nuclear weapons as the US nuclear force shrinks?
- Will US allies' foreign policies change in favor of nuclear neighbors, making the United States less secure?
- Is there an alternative other than nuclear protection that the United States can substitute?

This discussion identifies some of the players and future questions that must be considered in forging new nuclear arms reduction agreements, along with the dynamics in play within and among the nuclear nations. It is easy to understand why President Obama does not see a world free of nuclear weapons as happening within his lifetime. With the rapid spread of nuclear energy and weapons technology, we are about to enter a new world of arms negotiations much different from what we have practiced with the Russians. This means we may be on a path to reduce our weapons and delivery systems to levels closer to other nuclear-armed countries in the next decade or so. If this happens, we will then enter an era with multiple countries possessing relatively equal numbers of nuclear weapons, while others still seek to acquire nuclear weapons.

When we negotiate with these multiple nuclear powers in the future to bring our warhead numbers below 1,000 to around 500, we will be

negotiating less from the position of superior numbers and relative strength and more from relative parity. This will require a dramatic shift in the US national security outlook. Indeed, should such deep cuts be taken, we will have fewer warheads and delivery vehicles than we have had since the 1950s, and more countries will possess or be seeking to acquire nuclear weapons.

The Road to Zero

As discussed, the road to zero nuclear weapons is complex, with multiple actors, numerous and varying national security concerns, and dynamic and ever-changing internal national politics. There are many "suggestions" on how the world can get to zero, ranging from immediate unilateral disarmament by the United States to a new nonproliferation treaty where all nuclear countries sign a commitment to eliminate their nuclear weapons. The suggestions in the Shultz, Perry, and Kissinger article are a good place to start, but the discussion must continue and the thought be refined as time and conditions change. President Obama's commitment to "maintain a safe, secure and effective arsenal to deter any adversary, and guarantee the defense of our allies," suggests a graduated strategy of "momentum, to minimize, and marginalize," nuclear weapons.[40]

Momentum in a classical physics sense is mass times velocity. For this discussion the momentum of nuclear disarmament at the start of 2011 was zero, because until the new treaty took effect there was no inspection regime in place to ensure the two major nuclear powers were living by previous agreements. The first step toward returning momentum to the process is the New START. The positive effect of having in place accepted, verifiable inspection protocols is well worth the suggested reduction in nuclear warheads and delivery vehicles for both countries.

To add momentum, the two countries must bring tactical nuclear warheads into their nuclear arms negotiations, as recommended by the US Senate. By agreeing to minimize the number of these weapons through negotiations, we bring the entire nuclear arsenals of both countries to the table. Using established negotiation procedures, the United States and Russia can begin to first clearly define, then count, and ultimately set limits and inspection criteria for these weapons. Once all nuclear weapons are included in future nuclear arms reduction talks, more momentum can be added by including additional countries in the process.

With negotiation and inspection protocols established for all nuclear weapons as a foundational framework, the next two countries added to negotiations would be the United Kingdom and France. As nuclear members of NATO and close to the Russian homeland, these two countries can directly threaten Russia. By bringing in the UK and France, we can build trust with Russia to establish an acceptable balance of tactical and strategic nuclear warheads as we continue to minimize the numbers required by each side to around 1,000. To go below 1,000, the next biggest owner of nuclear weapons, China, would need to be brought into the negotiations.

To gain the trust of the Chinese, we must recognize them as full partners in the negotiations as NATO and Russia minimize their arsenals to approximately 500 tactical and strategic warheads. Momentum has been added to the process by adding the mass of new countries while maintaining velocity by continuing to reduce the overall number of weapons. With the five NPT signatories engaged in negotiations, it is time to start marginalizing the weapons.

The first step of marginalization would be a reaffirmation of the Nuclear Non-Proliferation Treaty with a commitment to move toward zero nuclear weapons, starting with all warheads not delivered by ballistic missile (currently defined tactical nuclear weapons and those delivered by long-range bombers). The next step would be for these countries, including the United States, to ratify the Comprehensive Nuclear Test Ban Treaty. This would prevent testing new capabilities, and over time, each country would begin to lose its nuclear expertise with regard to weapons design. Another move toward marginalization would be to share missile defense technology among these five nations. The advancement of missile defense technology is critical in providing security to our allies currently dependent on the US nuclear umbrella. With a commitment to reduce tactical nuclear weapons to zero, missile defense technology would become more effective, because it is most effective against ICBMs, SLBMs, and shorter-range ballistic missile delivery vehicles. With the five NPT signatories agreeing to acceptable negotiation and inspection standards, it is time to add more momentum by adding more countries.

The next countries to be added should be those with the technology and ability to create nuclear weapons but which have chosen to pursue a zero nuclear weapons policy. Such countries as South Africa, Brazil, and Japan would be brought into the process as monitors, offering nonnuclear countries representation at the negotiation tables to provide accountability and

incentive for those countries not to develop weapons. The next two nuclear countries to be added to the negotiations would be India and Pakistan. They need to be brought into negotiations together. To be part of the negotiations, they must accept the standards already established and become signatories to all previous treaties. India would be motivated to join this group for several reasons: first, the prestige of being recognized as a nuclear power by the world; second, if China has missile defense technology that neutralizes many of India's warheads, then India will want the same capability to protect itself. Pakistan should quickly follow suit for similar reasons. While getting Pakistan and India to negotiate will be a challenge, the addition of the next two countries, Israel and Iran, appears nearly insurmountable.

Through minimization and marginalization of nuclear weapons, the momentum of the major nuclear powers moving toward zero should provide the impetus for aspiring and supposed owners of nuclear weapons to join the negotiations. Because their ballistic nuclear arsenals would be susceptible to neutralization by the missile defense capability of surrounding countries, there would be less motivation to maintain a ballistic nuclear capability. The problem of getting these two countries in the same room will be challenge enough, but even this obstacle appears more achievable than working with the last nuclear power, North Korea.

North Korea will remain a special case until a change in leadership perhaps brings them back to normalized relations with the international community. Until that time, China will continue to have the preponderance of influence on North Korea and its nuclear arsenal. Six-party talks must resume and continue until North Korea can be brought into the greater international discussion of nuclear disarmament. With only a handful of nuclear weapons, North Korea remains part of the world's concerns, but it should not be a roadblock for the rest of the world to move toward zero.

Once all nuclear-armed nations are included in negotiations, efforts can begin to truly move the world to zero. With tactical nuclear weapons eliminated first and the major nuclear countries limited to 200–500 strategic nuclear warheads delivered by ballistic missiles, negotiations would focus on an inflection point. That inflection point is where there is an accepted balance of nuclear weapons that can be reduced to zero by all countries within a short period of time. For instance, if the NATO countries, Russia, and China were to reduce to a level of 250 strategic warheads each, they

may then rapidly agree to retire all their nuclear weapons, with all the other countries, within a couple of days. This would be the inflection point where instead of slowly reducing weapons over years, all weapons would be removed from service quickly. Once this inflection point is reached, inspection protocol and negotiations would need to continue, as it will take years for countries to completely dismantle all warheads. Monitoring and accounting of nuclear material produced by all nuclear powers will also need to continue, ensuring no country refines nuclear materials for weapons.

Compared to unilateral disarmament or a new grand treaty, which are suggested quick fixes to the nuclear disarmament challenge, this approach is a long process that incrementally builds momentum upon previous successes. This momentum is achieved by adding both "mass," or more countries to the negotiations, and "velocity," the deliberate act of reducing nuclear weapons in the world. Velocity is achieved by minimizing nuclear arsenals with an emphasis on eliminating tactical nuclear weapons first. Minimizing the numbers and types of nuclear weapons to hundreds of warheads delivered by ballistic missiles would allow further marginalization through shared ballistic missile defense technology. Additionally, eliminating nuclear weapons tests will reduce reliability and over time the skilled scientific force in nuclear design, limiting each country's capability to build new weapons. Nuclear weapons will also become marginalized by new technologies in warfare that cause less collateral damage, such as cyber warfare and lasers. The process of building momentum while minimizing and marginalizing nuclear weapons takes small but achievable steps toward moving the world to zero while maintaining an acceptable balance of power and deterrence capability among the many nations.

From this discussion it is obvious the concept of "momentum, minimization and marginalization" is not the panacea to solve the nuclear disarmament challenge. This approach does not directly address changing internal politics of each nation, except that the momentum of adding more countries to the process will make it more difficult for nations to renounce a ratified treaty. While it does not directly address all the concerns of allies currently under the US nuclear umbrella, it does confront a most important issue: tactical nuclear weapons.

Significance of Tactical Nuclear Weapons

While implementation of the New START will create momentum in the disarmament process, the first big challenge is minimizing tactical nuclear weapons. To understand this challenge we must understand the context in which we now operate. While other nuclear nations are upgrading their delivery systems and replacing old warheads, the United States has self-imposed a freeze on the replacement of its nuclear stockpile.[41] Also, because of its geographic location and historical context, its stockpile of nuclear weapons is considered strategic, while the preponderance of other nuclear weapons around the world are considered tactical. This is an important factor, as the New START only addresses strategic weapons, allowing Russia to retain an advantage in its tactical nuclear weapons inventory.[42]

As defined by the United States and Russia, the simple difference between strategic and nonstrategic or tactical nuclear weapons is the difference in the range of delivery vehicles. ICBMs, SLBMs, and long-range bombers with the intercontinental range to destroy military, industrial, and leadership targets in each other's homelands are considered strategic nuclear weapons. Those weapons not having the ability to reach the US or Russian heartlands when launched from the other's home soil are considered tactical nuclear weapons.[43] While there are some exceptions to this definition, it is important to realize that under the Strategic Arms Limitation Talks (SALT) I, SALT II, START, START II, the Strategic Offensive Reduction Treaty (SORT), and the New START, only strategic warheads and delivery systems (ICBMs, SLBMs, and long-range bombers) are considered. This excludes Russia's large nonstrategic weapons arsenal, estimated at 2,000 to 6,000 tactical nuclear weapons, from the negotiations.[44]

The actual number of Russian nonstrategic nuclear weapons is difficult to estimate. In its 2009 yearbook, *Armaments, Disarmament and International Security*, SIPRI places Russian operational numbers as few as 2,047 deployed tactical warheads. Of these, 701 are assigned to missile-defense interceptors. The remaining nonstrategic weapons are offensive, including 648 weapons for delivery by land-based bombers like the Tu-22M Backfire and Su-24 Fencer. Further, the Russian Navy possesses 237 tactical nuclear weapons to be delivered by naval aircraft and 276 on sea-launched cruise missiles. Another 185 tactical nuclear weapons are dedicated to antisubmarine warfare and surface-to-air missiles.[45]

These numbers are in contrast to the 400 US operational nonstrategic weapons—all B-61 gravity bombs delivered by fighters and bombers.[46] Excluding missile-defense warheads, the Russians have a three-to-one numerical advantage over the United States in tactical nuclear weapons. However, these shorter-range weapons, if based on Russian soil, cannot reach the continental United States. They would primarily concern states along Russia's periphery in Asia and Europe.

While the United States and Russia have negotiated an understanding and definition of strategic nuclear weapons, it is difficult for most countries in Europe and Asia to distinguish between Russia's strategic and tactical nuclear weapons. To countries like Estonia, South Korea, or Japan, one low-yield "tactical" nuclear weapon delivered by a missile or fighter aircraft would have devastating strategic implications.

These tactical nuclear weapons present additional challenges to negotiations and proliferation. They are, on average, smaller than strategic weapons and present multiple challenges. Smaller weapons are easier to hide, complicating verification of treaty limits. Unlike a bomber, ICBM, or SLBM force, tactical nuclear weapons are easily moved, contributing to counting and verification problems. Finally, the relatively low yield of some of these weapons may increase the likelihood of their use in certain crisis contingencies. This can improve deterrence effects but might also tempt decision makers to use them more readily.

Tactical nuclear weapons spread around the world put the United States in a difficult strategic position. If positioned near US territory, either clandestinely or on mobile platforms, these "tactical" weapons could become in effect, "strategic."

To move the discussion forward and include all nuclear countries, the definition of tactical and strategic nuclear weapons must be streamlined. A suggested modification would be the removal of range or ability to reach each other's homelands from the definition. A streamlined definition based on delivery vehicles would not change current agreements but would make the definition more relevant to all countries in future negotiations. Strategic nuclear weapons would continue to be identified as those delivered by any type of ballistic missile or bomber aircraft. All other nuclear weapons would be considered tactical, with the exception of Russia's nuclear missile defense, which should be included as a missile-defense capability. In follow-on negotiations, the United States must engage Russia on the issue of tactical nuclear weapons (not currently accounted for in

the New START). History demonstrates that when negotiating with the Russians, one must start from a position of relative strength. Unfortunately, the United States is currently at a numerical disadvantage, with some experts advocating an even weaker position.[47]

These experts argue that NATO should reduce its reliance on nuclear weapons and pursue a nuclear posture review ultimately leading toward nuclear disarmament.[48] While the goal is nuclear disarmament, the approach is short sighted. Russians traditionally take a zero-sum-game position in negotiations. If NATO unilaterally reduces its reliance on nuclear weapons, specifically forward-deployed US tactical nuclear weapons, there would be no immediate incentive for the Russians to reduce their arsenal. Conversely, the Russians would view this move as a sign of weakness and demand additional nonrelated concessions as incentives to reduce their tactical nuclear arsenal

Ultimately, the NATO summit in Lisbon last year took a typically multinational political approach of reaffirming its reliance on nuclear weapons for deterrence and defense, while committing to a strategic review of NATO's nuclear posture.[49] By maintaining a strong tactical nuclear capability in Europe, the United States can continue to provide a nuclear umbrella to its allies while presenting a bargaining chip for discussion with the Russians. This commitment to nuclear weapons as a deterrent is needed to engage the Russians in a discussion on reducing tactical nuclear arsenals. These force structure considerations will become critically important as the United States determines how it will configure its forces with an ever-shrinking nuclear arsenal.

Impact of Reductions on the United States in the Near Future

No matter what approach is taken in moving the world toward zero nuclear weapons, the path will be long and challenging. This time period will be dangerous, and the United States must be prepared to ensure its security by maintaining "a safe, secure and effective arsenal to deter any adversary, and guarantee the defense of our allies."[50] To maintain a safe, secure, effective arsenal, we must understand where we are and where we will be in the near future.

Upon implementation of the New START, the United States will find itself in a unique situation. Unlike Russia and China who have chosen to

modernize their nuclear arsenals, or countries like India, Pakistan, and Iran who have recently developed or are developing new weapons, the United States has chosen a path of "life extension" for its weapons.[51] This approach can be complicated, as some components originally developed for these weapons are no longer manufactured.[52] This new paradigm of parity in numbers, more nuclear nations, and an aging US arsenal will present numerous challenges to the United States over the coming decades.

First, moving below 1,000 strategic warheads and toward 500 or fewer delivery systems will require the Department of Defense to make difficult force structure decisions.[53] A reduction to the levels Russian president Dmitry Medvedev proposed in September 2009 would force the United States to look seriously at reconfiguring its current strategic triad of ICBMs, SLBMs, and long-range bombers, while considering the inefficiencies of maintaining three separate weapons systems in small quantities.[54]

There are numerous approaches the United States might take in apportioning its nuclear weapons and delivery systems. An in-depth study will be required to optimize deterrent effects of the US nuclear arsenal following any future arms treaties, but two general approaches will most likely be considered. The first is an across-the-board reduction in all weapons systems to include ICBMs, bombers, and SLBMs. Another more likely approach will be to completely eliminate one leg of the triad. Each leg possesses strengths and weaknesses and adds a certain element of deterrence that translates into retaliatory strength. If we look for guidance from other nations, such as Great Britain, that have trimmed their nuclear arsenals over the years, it appears SLBMs will be the weapons system of choice. The primary advantage of the SLBM force is its likely survivability from a surprise first strike. The downside is the "all of your eggs in one basket" syndrome. Advances in antisubmarine warfare may materialize in the future, threatening the survivability of US submarines. If so, the US preponderance in nuclear capability could be lost. Indeed, a single submarine malfunction might instantaneously bring its 24 missiles off alert.[55] If there were a defect in a missile or warhead type, then all US SLBMs could possibly be rendered useless. Therefore, it would be prudent for the United States to maintain some semblance of diversity in its nuclear arsenal.

Even though the Air Force is revitalizing its nuclear enterprise, the nuclear strategic bombing mission may be lost. While the secretary of defense committed to developing "a long-range, nuclear-capable penetrating bomber" in his 6 January 2011 Statement on Department Budget and

Efficiencies, it will be a while before the efficiencies are realized and the bomber is operational. During that time the aging US bomber fleet and a bomber on the drawing board would be easy force structure modification targets, either for "efficiencies" or negotiations. The loss of bombers would lead to a dyad of US nuclear weapons and eliminate an important signaling capability. Our bomber forces can signal willingness (an important part of deterrence) to use nuclear weapons and unlike other legs of the triad, bombers can be both launched and recalled. Without a bomber force, this traditional signaling mechanism could be lost. A potential solution is for Air Force fighters to assume more of this role.

To maintain some semblance of a triad and provide the necessary deterrence effects and security for our allies, the fighter community could ultimately pick up more of the airborne nuclear weapons delivery mission formerly provided by heavy bombers. With the new joint strike fighter becoming the Air Force's weapons system of choice, its mandated nuclear weapons delivery capability will be a vital part of its mission.[56]

As a joint strike fighter, the F-35 will also be flown by the US Navy. The Navy has maintained a strong nuclear infrastructure through its nuclear power plants and ballistic-missile submarine force. This expertise could be leveraged to provide a mobile tactical nuclear capability in times of crisis through carrier operations. Navy nuclear-capable joint strike fighters, flown from carriers, would eliminate foreign basing challenges. Another alternative in line with the Air Force chief of staff's call to "institutionalizing the thinking of the Air-Sea Battle concept," Air Force F-35 units could maintain tactical nuclear delivery capability and carrier qualifications.[57] In a time of crisis Air Force aircraft and weapons would be moved to carriers to demonstrate resolve and provide a signaling device.

In addition to interoperability between the Air Force and the Navy, many of our closest allies in Europe and Asia plan to purchase and fly the F-35. The ability to show resolve through F-35 nuclear deployment and delivery capability will deter potential adversaries and help provide a flexible, deployable nuclear deterrent critical to our US national defense.

While deterrence is the primary reason to maintain a reliable, visible nuclear force, a secondary effect of using the F-35 in a more robust nuclear role is the ultimate elimination of tactical nuclear weapons. The supportability of nuclear-capable fighters worldwide adds additional impetus to negotiate elimination of tactical nuclear weapons by all nuclear-armed countries. The ability to deploy globally, either to allied F-35 airfields or

onboard Navy carriers, would counterbalance the Russian navy's nuclear capability while also providing another bargaining chip for negotiating with Russia, China, and other countries on the reduction and eventual elimination of tactical nuclear weapons.

If F-35s are to play the nuclear-deterrent role traditionally filled by bombers, it would be wise to continue to deploy most of the estimated 200–350 forward-based nuclear bombs in NATO countries.[58] A firm commitment to this position by NATO would set the groundwork for negotiations with Russia on tactical nuclear weapons. This strategic shift away from a triad of ICBMs, SLBMs, and long-range bombers to one consisting of ICBMs, SLBMs, and deployable new fighters would solve the problem of the aging nuclear bomber fleet while maintaining the same deterrence capabilities inherent in an airborne force. At the same time this move would add momentum to the discussion of tactical nuclear disarmament. Bringing tactical nuclear weapons to the negotiating table is the first real step toward true nuclear disarmament.

Conclusion

In April 2009, President Obama set the nation on the path toward the eventual long-term goal of zero nuclear weapons. Nuclear disarmament has been a worldwide goal since the Nuclear Non-Proliferation Treaty was opened for signature in 1970. Over the years, states have taken numerous positive steps toward that end, with the New START further reducing both the US and Russian nuclear arsenals. Perhaps in later rounds, after the current treaty, the two sides may agree to levels below 1,000 strategic warheads. Crossing the 1,000 threshold will open a new, more complicated era of nuclear arms negotiations.

It will take time to understand the different players, motives, and issues each new country brings to the table. The challenge is to coordinate the step-by-step disarmament of the nine current members of the nuclear weapons club while simultaneously attempting to dissuade others from "going nuclear." New challenges on the path to zero may emerge as allied nations consider acquiring nuclear weapons to make up for a perceived loss of US umbrella protection or as other nations see an opportunity to increase their relative military and political power and prestige.

To counter these unintended consequences, it is important to negotiate with all of the world's nuclear-armed nations through a process of building

momentum on previous successes by minimizing the number of nuclear warheads while ultimately marginalizing their utility. However, even if all nuclear-armed nations begin negotiations today, total disarmament will require a long time. During this protracted period of negotiations, we will find ourselves in a world with a group of countries that possess a relatively large and growing number of nuclear weapons.

The preponderance of weapons in this new environment will be so-called nonstrategic or tactical nuclear weapons maintained primarily by Russia. This imbalance will present a different dimension to the US national security posture and force structure. The United States will have to make tough choices as negotiations further limit delivery vehicles and warheads. With bombers the most likely losses to the strategic retaliatory forces, the Air Force will need to focus more on its tactical nuclear mission. Also, the Navy could pick up an airborne nuclear delivery capability under the new air-sea battle concept that would resolve many of the current bomber and forward land-basing issues.

The United States has embarked on a path to a nuclear-free world. Its challenge is finding a path that maintains an acceptable balance of power between nations while providing an appropriate level of deterrence. Any realistic path will be fraught with unknown challenges, numerous new actors, and dynamics that will yield surprises while moving toward the ultimate goal of national security and total nuclear disarmament. **SSQ**

Notes

1. "Remarks by President Barack Obama, Hradcany Square, Prague, Czech Republic," Office of the Press Secretary, The White House, 5 April 2009, http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered.

2. George Shultz, William J. Perry, Henry A. Kissinger, and Sam Nunn, "Toward a Nuclear-Free World," *Wall Street Journal*, 15 January 2008, http://online.wsj.com/public/article_print/SB12003642267358 9947.html.

3. "Remarks by President Barack Obama."

4. "The New START Treaty and Protocol," The White House Blog, 8 April 2010, http://www.whitehouse.gov/blog/2010/04/08/new-start-treaty-and-protocol.

5. US Department of State (DoS), "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)," entered into force 5 March 1970, *United States Treaties and Other International Agreements*, vol. 757, no. 10485, http:// www.state.gov/t/isn/trty/16281.htm.

6. Isaac Asimov, *Understanding Physics* (New York: Walker, 1966), 34.

7. The Heisenberg uncertainty principle simply states that one cannot know the position and momentum of an atom simultaneously. Similarly, under the current international environment, no country or entity completely knows the "nuclear position" or the "direction and speed" (momentum) a country is moving with regards to nuclear weapons. Richard Rhodes, *The Making of the Atomic Bomb* (New York: Simon & Schuster, 1986), 130.

8. James Schlesinger, chairman, *Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management: Phase I: The Air Force's Nuclear Mission* (Washington: DoD, 2008).

9. DOS, "Treaty on the Non-Proliferation of Nuclear Weapons."

10. Merle David Kellerhals Jr., "U.S. Senate Ratifies New START Treaty," *America.gov*, 22 December 2010, http://www.america.gov/st/peacesec-english/2010/December/20101222163224 elrem0.7087824 .html?CP.rss=true.

11. Greg White, "Russia Fears 'Reset' of Relations with U.S.," *Washington Wire*, 3 November 2010, http://blogs.wsj.com/washwire/2010/11/03/russia-fears-reset-of-relations-with-us/.

12. Dmitry Astakhov, "President Medvedev welcomes START treaty ratification by U.S. Senate (Update 1)," *RIA Novosti*, 23 December 2010, http://en.rian.ru/russia/20101223/161896483.html.

13. Ibid.

14. Fred Weir, "With Russian ratification of New START, what's next for US-Russia relations?" *Christian Science Monitor*, 26 January 2011, http://www.csmonitor.com/World/Europe/2011/0126/With -Russian-ratification-of-New-START-what-s-next-for-US-Russia-relations.

15. US Mission, "Remarks by Clinton, Russia's Lavrov at New START Event," 5 February 2011, http://geneva.usmission.gov/2011/02/07/clinton-lavrov-start-treaty-signing/.

16. DoS, "START II Treaty," 1997, http://www.state.gov/www/ global/arms/starthtm/start2 /st2intal.html.

17. "Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Weapons," 3, 8 April 2010, http://www .state.gov/documents/organization/140035.pdf.

18. Schlesinger, *Report of the Secretary of Defense*, 18.

19. "Russia Air Force to Get New TU-160 Strategic Bomber in April," *RIA Novosti*, 22 April 2008, http://en.rian.ru/russia/20080422/105640820.html; and "Russia to Start Construction of 4th *Borey*-Class Sub in December," *RIA Novosti*, 5 October 2009, http://en.rian.ru/russia/20091005/156357397 .html.

20. Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook 2009: Armaments, Disarmament and International Security* (Oxford, UK: Oxford University Press, 2009), 353.

21. For an in-depth study of US and Russian nonstrategic or tactical weapons, see Amy F. Woolf, *Nonstrategic Nuclear Weapons* (Washington: Congressional Research Service, 2009), 14–17.

22. Stephen J. Cimbala, "Forward to Where? U.S.–Russia Strategic Nuclear Force Reductions," *Journal of Slavic Military Studies* 22, no. 1 (January 2009): 68–86, http://www.informaworld.com/smpp /ftinterface~db=all~content=a909097059~fulltext=713240928.

23. SIPRI, *SIPRI Yearbook 2009*, 364.

24. Office of the Secretary of Defense, *Annual Report to Congress, Military Power of the People's Republic of China 2009*, 24, http://www.cfr.org/publication/18943.

25. Hans M. Kristensen, "Estimated Nuclear Weapons Locations 2009," *FAS Strategic Security Blog*, November 2009, http://www.fas.org/blog/ssp/2009/11/locations.php.

26. States with vulnerable nuclear forces may be tempted to launch their forces on warning (LOW) or launch under attack (LUA), and this could put a hair trigger on these weapons to prevent their being destroyed by surprise attack. The Chinese seem to have solved this "use or lose" dilemma by deploying nuclear arms underground.

27. SIPRI, *SIPRI Yearbook 2009*, 359.

28. Ibid., 360.

29. Elliott Francis and Michael Evans, "Britain's Nuclear Overture—We Will Cut Trident Fleet," *Timesonline* (London), 22 September 2009, http://www.timesonline.co.uk/tol/news /politics/article6845247.ece.

30. SIPRI, *SIPRI Yearbook 2009*, 360.

31. Edward Cody, "After 43 Years, France to Rejoin NATO as Full Member," *Washington Post*, 12 March 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/03/11 /AR2009031100547.html.

32. SIPRI, *SIPRI Yearbook 2009*, 367, 370.

33. Ibid., 367, 372.

34. Rolf Mowatt-Larssen, "Nuclear Security in Pakistan: Reducing the Risks of Nuclear Terrorism," *Arms Control Today*, July/August 2009, http://www.armscontrol.org/act/2009_07-08/Mowatt-Larssen.

35. SIPRI, *SIPRI Yearbook 2009*, 375.

36. Schlesinger, *Report of the Secretary of Defense*, 18.

37. Federation of American Scientists, "Nuclear Weapons Program," WMD around the World, 16 April 2000, http://www.fas.org/nuke/guide/japan/nuke.

38. Joseph Cirincione, *Bomb Scare: The History and Future of Nuclear Weapons* (New York: Columbia University Press, 2007), 103.

39. Jun Hongo, "Probe Launched into Four Secret Pacts with U.S.," *Japan Times online*, September 2009, http://search.japantimes.co.jp/cgi-bin/nn20090926a2.html.

40. "Remarks by President Barack Obama."

41. Jeffrey Lewis, "After the Reliable Replacement Warhead: What's next for the U.S. Nuclear Arsenal?" *Arms Control Today*, December 2008, http://www.armscontrol.org/act/2008_12/Lewis.

42. Woolf, *Nonstrategic Nuclear Weapons*, 14–16.

43. Ibid., 5.

44. Ibid., 17.

45. SIPRI, *SIPRI Yearbook 2009*, 354.

46. Ibid., 348.

47. Arms Control Association, "Experts Urge NATO Ministers to Rething Alliance Nuclear Policy," news release, 11 October 2010, http://www.armscontrol.org/print/4483.

48. Oliver Meier and Paul Ingram, "A Nuclear Posture Review for NATO," *Arms Control Today*, October 2010, http://www.armscontrol.org/act/2010_10/Meier-Ingram.

49. "Lisbon Summit Declaration," *NATO*, 20 November 2010, http://www.nato.int/cps/en/natolive/official_texts_68828.htm.

50. "Remarks by President Barack Obama."

51. William J. Perry, chairman, and James R. Schlesinger, vice- chairman, *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington: US Institute of Peace Press, 2009), 40, http://www.usip.org/strategic-posture-commission/view-the-report.

52. Ibid.

53. Joint Working Group of the American Association for the Advancement of Science (AAAS), American Physical Society, and the Center for Strategic and International Studies, *Nuclear Weapons in 21st Century U.S. National Security* (Washington: AAAS, 2008), 8, http://www.aps.org/policy/reports/popa-reports/upload/nuclear-weapons.PDF.

54. President Medvedev stated on 24 September 2009 that the United States and Russia were discussing the possibility of slashing nuclear weapons delivery vehicles by 67 percent. From the US State Department report in April, the United States has 1,198 delivery vehicles; this cut would reduce US delivery vehicles to below 500. "Russia, U.S. to Slash Nuclear Delivery Vehicles—Medvedev," *RIA Novosti*, 24 September 2009, http://en.rian.ru/world/20090924/156243233.html.

55. "Trident Fleet Ballistic Missile," US Navy Fact File, *Navy.mil*, 17 January 2009, http://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1400&ct=2.

56. Adam J. Hebert, "New Nukes, Old Nukes," *Air Force Magazine* 92, no. 10 (October 2009): 20.

57. Reed, "USAF Needs New Long-Range Bomber."

58. Ian Anthony, *The Future of Nuclear Weapons in NATO* (Stockholm: SIPRI, 4 February 2008), 28.

The Sources of Instability in the Twenty-First Century

Weak States, Armed Groups, and Irregular Conflict

Richard Shultz, Roy Godson, Querine Hanlon, and Samantha Ravich

The world has changed! It has become more complex, with shadowy and seemingly unpredictable conflicts taking place around the globe. But there is a pattern to these fights. They are not unpredictable but discernable. The sources of instability in the twenty-first century's international security environment will largely result from a proliferation in the number of weak and failing states as well as powerful armed groups, some of which are able to affect fundamental security by causing major geopolitical damage in their own states, in various regions, or to the United States itself. Moreover, this proliferation creates new interactions and interrelationships between and among local, regional, and global players. These developments, in turn, are fostering the emergence of partnerships and coalitions comprised of armed groups, other nonstate actors, and authoritarian revisionist states. These formal and informal groupings employ an array of irregular violent and nonviolent means to extend their power and influence. A persistent and enduring pattern of irregular conflict is observable, and it will continue well into the twenty-first century. Faced with these security

---

This article was prepared under the auspices of the National Strategy Information Center (NSIC). It is drawn from NSIC's new book, *Adapting America's Security Paradigm and Security Agenda* (Washington: NSIC, April 2011. The volume examines how instability, conflict, and war in the twenty-first century have changed in significant ways; highlights how those changes challenge the United States and other democracies; and identifies specific capabilities that the United States and its allies need to develop to manage and mitigate the threats emerging from this new environment. More information on NSIC and its Project on Adapting America's Security Paradigm and Security Agenda can be found at www.strategycenter.org.

Richard Shultz is professor and director, International Security Studies Program at the Fletcher School, Tufts University; Roy Godson is president of the National Strategy Information Center and emeritus professor of government, Georgetown University; Querine Hanlon is dean of academic affairs and associate professor of the College of International Security Affairs, National Defense University; Samantha Ravich is former deputy national security advisor to the vice president of the United States.

challenges, democratic states will likewise need to foster their own coalitions of both state and nonstate allies to oppose them. This article provides the broad contours of these developments through the lens of real-world cases.[1] In a 1997 speech, the commandant of the Marine Corps, Gen Charles Krulak, warned that conflict and war in the future would be different from the conventional contingencies the Pentagon was prepared to fight. Titling his speech "Not like Yesterday," he counseled that this conventional mind-set could lead to military misfortunes: "[O]ur enemies will not allow us to fight the son of Desert Storm, but they will try to draw us into the stepchild of Chechnya. Our most dangerous enemies will challenge us asymmetrically in ways against which we are least able to bring strength to bear—as we witnessed in the slums of Mogadishu."[2]

General Krulak was considered way out of step by the other joint chiefs, the DoD bureaucracy, and the services. They did not think about or prepare for the conflicts he foresaw. Those irregular fights were considered at best tertiary security matters—internal disturbances, criminal enterprises, or ethnic group rivalries—of little interest to those US security institutions responsible for the conduct of warfare, diplomacy, and intelligence.[3]

The conflicts Krulak saw emerging in the 1990s burgeoned in the years following 9/11. As they did, other former general officers and officials came to the same conclusions. Consider Gen Rupert Smith, deputy SACEUR from 1998 to 2001. During his career in the British Army, he trained to fight twentieth-century "interstate industrialized war." But in the Cold War's aftermath, General Smith had to deal with conflicts that diverged considerably from that standard in Northern Ireland, Bosnia, and Kosovo. Then, in retirement, he witnessed the 9/11 attacks, the wars in Afghanistan and Iraq, and al-Qaeda's transnational operations.

Smith had seen enough. In his 2006 book, *The Utility of Force: The Art of War in the Modern Age*, he declared: "It is now time to recognize that a paradigm shift in war has undoubtedly occurred: from armies with comparable forces doing battle *to* a strategic confrontation between a range of combatants . . . using different types of weapons, often improvised." Twentieth-century conventional war was being replaced by the new paradigm of "war amongst the people." And those conflicts, said Smith, "can take place anywhere: in the presence of civilians, against civilians, in defense of civilians."[4] Critical to making sense of this new state of affairs, he implied, was realization that wars between nation-states, all too common in the twentieth century, were becoming anomalies.

The idea that there was a paradigm shift in the conduct of conflict and war found its way into the US Department of Defense (DoD) in 2006. The 2006 iteration of the *Quadrennial Defense Review* (*QDR*)—the Pentagon's legislatively mandated every-four-year assessment of the strategies, capabilities, and forces the United States needs to manage today's conflicts and tomorrow's threats—asserted that irregular warfare had become a vital mission area and the services needed to become prepared for it. Post–9/11 combat was depicted as "irregular in its nature." Enemies in those fights were "not conventional military forces" belonging to nation-states. Rather, they included various armed nonstate actors who employed indirect and asymmetric means.

The 2006 *QDR* also set in motion irregular warfare initiatives inside the DoD leading to the December 2008 release of DoD Directive (DoDD) 3000.07, *Irregular Warfare* (*IW*). That directive was unambiguous about twenty-first-century conflict, declaring: "Irregular warfare is as strategically important as traditional warfare . . . [and it is essential to] maintain capabilities . . . so that the DOD is as effective in IW as it is in traditional [conventional] warfare." Moreover, for DoDD 3000.07 the capabilities required for each type of fight were different.[5]

What this all adds up to is the basic fact that today's world cannot be understood through the lens of the twentieth-century security paradigm. The nature of instability, conflict, and war has evolved dramatically beyond conventional fights between the armies of nation-states. An examination of conflict trends since the end of the Cold War provides empirical evidence of a prevalent and enduring pattern of irregular conflict and instability.[6] These trends constitute a pervasive part of a complex twenty-first-century international security environment in which violence, conflict, and war differ markedly from the ways in which the United States and other major states thought about and prepared for armed discord during most of the twentieth century.

There is little to suggest that this will change any time soon. This trend is here to stay for the foreseeable future. It constitutes the prevalent pattern of instability, and it will continue. To be sure, conventional war between states is still possible, but that will be more of an anomaly.

Characteristics of the Twenty-First-Century Security Environment

Given these developments, what are the particulars—the details—of the differences, new complexities, and changed conditions that characterize twenty-first-century instability, conflict, and war? And why are these developments not temporary disruptions or short-lived distractions but symptoms of a new security environment?

To answer these questions one must highlight the broad contours and present the big picture of these developments. The twenty-first-century security environment will, at minimum, be characterized by the following dimensions:

- A proliferation in the number of weak and failing states as well as powerful armed groups will be able through violent and nonviolent means to affect stability and security at the local, regional, and, in some instances, even global levels.
- This proliferation of actors creates new interactions and interrelationships between and among local, regional, and global players.
- These first two developments, in turn, foster the emergence of coalitions that will be comprised of states, armed groups, and other nonstate actors. These formal and informal groupings, to achieve their aims, employ irregular warfare tools and techniques.
- Faced with the security challenges of these hostile coalitions of actors, democratic states are beginning to foster coalitions of state and nonstate allies to oppose them.

To begin to decipher and illustrate these developments and their interplay, each of these dimensions will be examined and illustrated through the lens of real-world situations and events.

Weak/Failing States and Burgeoning Armed Groups

The proliferation of weak and failing states will be among the preponderant sources of instability over the next decade or two, at the very least. To varying degrees, these kinds of states are unable to control all their territory, maintain a monopoly over the instruments of force, or perform core functions, beginning with providing security for significant sections of their populations. Moreover, they also suffer from high degrees of

corruption. When these conditions become severe, a state's legitimacy seriously erodes and it may even vanish.

Several research and policy-oriented institutions over the last number of years have developed analytic measurements for assessing the capacity and viability of today's approximately 195 states in the world. What their analysis has found is the majority of those states are weak, failing, or failed. Here is the breakdown, drawn from those appraisals: [7]

	Democratic	Authoritarian
Strong States	40 to 45	10 to 15
Weak States	50 to 55	30 to 35
Failing/Failed States	10 to 20	

The conditions that contribute to state weakness and failure also provide the setting for armed group incubation and maturation.

Consider the regional security challenges posed by weak states in Mesoamerica—the territory stretching from Mexico through Central America and the Caribbean Basin to Colombia. Most states there are weak democracies, and that weakness manifests itself in several ways. First, large segments of the urban and rural populations of these states have little confidence in their governments. Many believe government is corrupt, incompetent, and unable to improve their lives or protect them from violence. To survive, they turn to the informal economy and are susceptible to the blandishments of criminal activities, gangs, and other types of organized crime.[8]

These states are also weak because their governments just barely control their cities; outside these urban areas, that control is much weaker. To varying degrees rural areas and even parts of cities, particularly in Colombia and Mexico, have limited government presence and authority. With few exceptions, the police and security forces of the region have limited capabilities. Salaries are low, training and equipment are insufficient, and turnover tends to be high. There is corruption from near the top on down. This has, in some instances brought the military into the security situation. But they too suffer from some of the same weaknesses prevalent in the police and other security forces.[9]

As noted above, where weak states exist, armed groups may emerge and take root.[10] Again, consider Mesoamerica. In Mexico the major armed groups—the Gulf, Tijuana, Juarez, and Sinaloa cartels—are sophisticated and powerful actors, employing thousands and effectively competing for power with the Mexican state.[11] They have well-armed, murderous para-

military forces employing hundreds of former Mexican military and policemen. In 2008 they assassinated over 5,000. The cartels corrupt and terrorize large numbers of state, municipal, and rural elected officials, police chiefs, and important local leaders so they can go about their business with relative impunity.[12]

The interplay between weak states and armed groups—the first dimension identified above—can be found in other parts of the world as well. Following the March 2003 invasion of Iraq, they came together to foster a complex, protracted, irregular war that the United States neither anticipated nor was prepared to fight.[13]

Iraq's disparate sectarian, ethnic, and tribal divisions were held together by Saddam Hussein through repression. The regime was a police state. With its removal, Iraq devolved into a weak state where the central government in Baghdad had neither the legitimacy nor the power to control the diverse regions. And the United States had too few troops to establish stability and the wrong doctrine for doing so. Chaos, internal conflict, and societal breakdown ensued, as armed groups burgeoned. Insurgent, terrorist, militia, and criminal groups opposed coalition forces and also sought to weaken each other.[14]

These included Sunni "nationalist" and "Islamist" insurgents. The former were initially dominated by regime loyalists, mainly members of Saddam's security and intelligence services. They were quickly joined by fighters from Sunni tribal confederations. Sunni insurgents were also comprised of homegrown Salafi jihadists. They were joined by their internationalist counterparts when bin Laden called on these warriors to join the fight. At the same time, two major Shia armed groups emerged—Moqtada al-Sadr's Mahdi Army and the Badr Corps of the Supreme Council for Islamic Revolution. Finally, armed criminal groups flourished.[15]

A third example of this weak state-armed group juncture is displayed in different parts of Nigeria to include the Niger Delta, the critical oil-producing region. Armed groups emerged there in the early 1990s due to growing tensions between foreign oil corporations, the Nigerian government, and minority ethnic groups who felt they were being exploited. This violence intensified throughout the 1990s and continues in the twenty-first century.

In spite of vast oil wealth, parts of Nigeria have several characteristics of a weak state.[16] For example, a large segment of the delta's population has little or no confidence in the government. Petroleum riches have not trickled down to the majority of the population. Official corruption is viewed as a

way of life. The people of the delta are poorer than they were in the 1960s. Population density is among the highest in the world, expanding at 3 percent per year. The same is not true of economic growth and jobs.[17]

Additionally, the Nigerian government's military and security forces are unable to achieve control across this important delta region. When combined with official neglect and environmental degradation caused by energy projects, the end result is social unrest and political violence generated by armed groups.[18]

Composed of young men dissatisfied with their inability to find jobs, armed groups began appearing in the delta in the 1990s. By the early years of the twenty-first century, the most powerful one operating there was the Movement for the Emancipation of the Niger Delta, or MEND. Its attacks on oil pipelines and other oil facilities have reduced oil output considerably. MEND is much stronger than its predecessors, employing more sophisticated tactics.[19]

For example, in June 2008, MEND fast boats attacked the Shell-operated Bonga oil platform, shutting down 10 percent of Nigeria's oil production for two months. The oil platform, capable of extracting a massive 200,000 barrels of oil a day, was assumed to be outside MEND's reach due to its location 120 km offshore. This attack demonstrated a new level of power projection and put all of Nigeria's oil platforms within range of MEND forces.[20]

In early September 2008, MEND proclaimed it was launching an "oil war" throughout the Niger delta.[21] Oil companies, the Nigerian government, and the United States (Nigeria is its fifth largest supplier of oil) are greatly concerned about MEND's ability to disrupt global oil supplies.

New Interrelationships among Local, Regional, and Global Players

These developments in Mexico, Iraq, and Nigeria did not take place in isolation from the rest of the world. They cannot be characterized as local security problems. Rather, they transpired within a broader context that encompasses the second dimension of the twenty-first-century security environment—*the proliferation of actors has created new interactions and interrelationships between and among local, regional, and global players.* In each of the examples of the interplay between weak states and armed groups in Mexico, Iraq, and Nigeria, one can observe how that interplay

creates new interactions and interrelationships—both cooperative and adversarial—between local actors and other regional and global players.

Mexico's armed groups, including the Gulf, Tijuana, Juarez, and Sinaloa cartels, interact, engage, and form cooperative relationships with other forms of organized power in the Central American region. These include criminal gangs that, like the cartels, seek to undermine weak democracies in Central America to carry out their illicit activities with impunity. Perhaps the most dangerous of these gangs are the Maras.[22]

The Maras have evolved from first-generation street gangs into second-generation, business-oriented criminal groups able to control the commerce and streets of urban areas in El Salvador, Guatemala, and Honduras, to third-generation, criminal organizations that have established networks extending from Central America into US cities. Through these networks the Maras have the potential to move illicit goods across borders to include the United States. And, if profitable they could make these networks available to other criminal enterprises operating out of Mesoamerica, and beyond.[23]

Armed groups in Iraq likewise have established networks and cooperative relationships with various regional actors. For example, Syria has provided a crucial logistical hub and served as a sanctuary for leaders of various Sunni armed groups. In addition, their financial networks, in part, run through Syria. For Damascus, this interaction with Sunni armed groups is a way of fighting asymmetrically with the objective of helping turn Iraq into a quagmire for the United States.[24]

There is evidence that other Arab states have established cooperative relationships with Sunni insurgents in their bid to frustrate Iranian influence in Iraq.[25] And, Tehran has sought to extend its power through engagement with both Moqtada al-Sadr and the Supreme Council for Islamic Revolution (now known as the Islamic Supreme Council of Iraq). In the case of the former, Iran provided financial and military support to the Mahdi Army. This included a sophisticated IED that fires a molten slug capable of penetrating US armored vehicles.[26]

Interrelationships between local armed groups and elements of the international Salafi Jihad movement can be seen in Iraq. Al-Qaeda in Iraq (AQI) received support through the constituent parts of al-Qaeda's (AQ) global movement, including websites and mosques. AQ facilitators assisted in the recruitment and travel of jihadist militants to Iraq. Captured AQI records of 700 foreign fighters who entered Iraq between 2006 and 2007

revealed that 41 percent came from Saudi Arabia and 18 percent from Libya, while Syria, Yemen, Algeria, and Morocco each accounted for 6 to 8 percent. AQI also received financial assistance from wealthy sheiks from the GCC states sympathetic to radical Islamism.[27]

Beyond Iraq, an unpacking of the al-Qaeda and Salafi Jihad network provides a paramount illustration of how the interplay between weak states and armed groups fosters interrelationships between local, regional, and global actors. Al-Qaeda's founders sought to establish the organization as the vanguard of a global movement. It summoned a broad universe of like-minded extremists to become part of a global network to fight near enemies—apostate Muslim regimes—and the far enemy, the United States.

In the latter 1990s, in Afghanistan, AQ built a network of linkages with a score of national-level Islamist groups who were employing guerrilla violence and terrorism against their governments. These included ones in Algeria, Morocco, Egypt, Uzbekistan, Chechnya, Kashmir, Indonesia, the Philippines, and Bosnia. In its Afghan sanctuary, AQ provided financial assistance, training, weapons, and spiritual guidance to their fighters. It also carried out global attacks on the United States in East Africa, Yemen, and elsewhere.[28]

Al-Qaeda's network was set back considerably with the loss of its Afghan sanctuary in 2001. To adapt, it sought to reestablish linkages with local Salafi Jihad groups, in part through creation of an Internet-based virtual sanctuary that could disseminate official communiqués, doctrinal treaties, strategy and operational documents, and training videos.[29] AQ also adapted by taking advantage of ungoverned territory to reestablish its physical sanctuary within another weak state—Pakistan.[30]

MEND's attacks on delta oil facilities reach across the globe to negatively impact the industrialized world. To undermine the Nigerian government, MEND targets the oil industry with sophisticated means. It has the resources to purchase advanced weapons, such as fast boats used to shutdown the Bonga oil platform.

How do they acquire these capabilities? From another category of nonstate actors who are likewise a part of today's security context—super-empowered individuals, groups, and institutions.[31] Operating separately, or at times through or aligned with armed groups, these micro actors have the capacity to affect the security environment by facilitating conflict and instability. Their power flows from personal wealth, financial or other material resources and technologies, access to weapons, or their ability to influence directly or serve

as a conduit for influence. In the case of MEND, this interaction was with black-market arms dealers who could deliver fast boats.

These attacks disrupt Nigerian oil production. Targets are systematically selected to stop production or delay or halt repairs. Given the impact on the world oil market, the Nigerian government has sought the help of regional and global actors. It has asked the United States and the United Kingdom to provide assistance to its military, a request to which both countries agreed.[32]

Emerging Coalitions of States, Armed Groups, and other Nonstate Actors

The first two dimensions discussed above, in turn, foster the final one—*the emergence of coalitions comprised of states, armed groups, and other nonstate actors that employ irregular tools and techniques to achieve their aims.* These pacts can range from formal to de facto coalitions to loose affiliations. And they can be found at the local, regional, and global levels.

One region that is quite illustrative of this complex interplay of state and nonstate actors is the Levant—particularly in Lebanon, the Palestinian territories, Israel, in and around Syria, but also encompassing Iran. The Levant is host to many interconnected actors, including de facto coalitions between states and a myriad of armed groups and their associated political movements that seek to undermine the sovereignty and legitimacy of other states in the region. This is reflected, for example, in the de facto coalition arrangements that exist among Syria, Iran, Hezbollah, and Hamas.

Syria has formed alliances with several armed groups in the Levant to extend its power and influence. In Lebanon, which Damascus has long considered a de facto part of Syria, it does so through several means to include collaboration with Hezbollah. This arrangement also allows Syria to fight Israel through asymmetrical means.[33] Of course, Tehran remains a major collaborator and benefactor to Hezbollah, and this has been the case since its emergence in the early 1980s.[34] Indeed, it was Iranian weapons that assisted Hezbollah considerably in its short war with Israel in the summer of 2006.[35]

Support from Iran and Syria has enabled Hezbollah to strengthen dramatically its clandestine apparatus and war-fighting capabilities. As a result, it has emerged as a powerful nonstate actor throughout the Levant and beyond.[36]

In the Palestinian territories Syria has also for many years facilitated the operations of several armed groups as another way of fighting Israel through indirect means. In the past these have included the Popular Front for the Liberation of Palestine (PFLP) and the Democratic Front for the Liberation of Palestine (DFLP), each of which maintains command centers in Damascus. Since the second Intifada began in 2000, Syria's most important armed group ally in the territories is Hamas, which has become the de facto ruler in Gaza. It has established various overt and covert security, intelligence, and paramilitary forces, which it employs to fight against Fatah, its Palestinian counterpart, and to attack Israel. Iran likewise uses its various clandestine organizations to indirectly provide external material support and military equipment to Hamas.[37]

Finally, a complex array of other armed movements and clandestine organizations operate in the Levant and associate with al-Qaeda and the Salafi Jihad movement. For example, in Lebanon self-styled al-Qaeda affiliates are now operating out of Palestinian refugee camps. Perhaps the best known is Fatah al-Islam, which subscribes to bin Laden's ideology of war against non-Muslims—specifically the West and Israel. In 2007, it fought pitched battles for over five months with the Lebanese army. Similar groups have emerged in the Palestinian territories, including the Army of Islam in the Gaza Strip. It is ideologically affiliated with the global jihad and has adopted its modus operandi, including the abduction of foreigners and attacks on targets identified as damaging Islamic morals such as Internet cafés.

Opposition Coalitions of Democratic States and Nonstate Actors

Faced with the security challenges of hostile coalitions and multiple actors, democratic states likewise have begun to foster coalitions of both state and nonstate allies to oppose them. In the Levant to counter these hostile forces, Israel has sought to bring together de facto coalitions of allies and partners that include both like-minded democratic states and those who in the past it has fought. Moreover, Israel has reached out to actors beyond the Levant to do so.

In terms of like-minded democratic states, most important for Israel is its long-standing partnership with the United States. But there are other democracies as well that Israel has formed security arrangements

with to counter elements of the array of hostile forces aligned against it in the Levant region. For example, while they have their differences, there are several security issues that serve as the basis for cooperation between Israel and India.[38] These include intelligence and military cooperation against Salafi Jihad terrorism. While counterterrorism remains the greatest area of cooperation between the two countries, they share other security concerns that facilitate a growing strategic relationship. For example, the safety of Pakistan's nuclear weapons stimulates Indian-Israeli defense and security cooperation.

Beyond like-minded democracies, Israel also engages other actors in the region. For example, it has given some assistance to Fatah, identifying and/or capturing members of the Hamas clandestine infrastructure that seeks not just to control Gaza but the West Bank as well. In doing so, Israel seeks to prevent Hamas from emerging as the dominant force in the West Bank.

Of course Israel is not the only democratic state that has sought both state and nonstate allies as a result of multiple hostile actors arrayed against it. Another case in point is Mexico. As noted earlier, Mexico is engaged in an increasingly violent internal struggle against heavily armed criminal cartels that have intimidated the public, corrupted law enforcement institutions, and created an environment of impunity to the law. The Calderon administration is confronted by criminal syndicates that have subverted state and municipal authorities and present a major danger to stability and the rule of law across Mexico.[39]

In Mexico there are two emerging coalitions vying for dominance in various parts of the country. One consists primarily of diverse armed groups that are mostly criminal.[40] They prey on the local population and exploit Mexico's geographical advantage of transit between the Caribbean, Central America, and the market of the United States. It is estimated that 20 million Americans buy illegal drugs monthly, and $15–25 billion in narco-trafficking profits are pumped back into Mexico annually in cash and arms.[41]

Most attention is focused on four major cartels and their violent battles for control of the drug trade, their penetration of Mexican politics at the state and federal levels, and their horrific paramilitary and terrorist violence against soldiers, police, and judicial officials to secure impunity.[42] They also maintain connections with narco-traffickers across Mesoamerica and beyond, even into West Africa.[43] There are also many other similar criminal

groups, less well organized, who also recruit local police and judicial authorities and terrorize the local population with systemic kidnapping, extortion, robbery, money laundering, trafficking in drugs, and smuggling of people, counterfeit and stolen goods, and arms.[44]

The temporary coalitions these criminal cartels form have few if any formal agreements. They trade with and extort one another and have created an alternative security structure and "rules" that compete with those of the government at the local level in many parts of the country and in important sectors of society. They also seek influence in Central America, in the US–Mexican border region, and in some US cities. Hostile state and nonstate actors from outside the Western Hemisphere have also sought opportunities to enter into coalitions with these armed groups to further their own interests.[45]

Another set of coalitions that supports democratic society and is opposed to criminality and its abuse of the security and police institutions of the Mexican state has begun to surface. It is led by Mexico's top elected federal officials and the governors of most states. However, as one descends the bureaucratic chain of federal, state, and municipal officials, the integrity of much of security and law enforcement personnel and institutions is more problematic and quite susceptible to intimidation and corruption.

The United States seeks to support the leaders of the Mexican federal and state security establishments and to bolster their institutions. There are a variety of formal agreements with the Mexican authorities that receive over half a billion dollars each year. Most US support is focused on neutralizing the power and programs of the major cartels and of other transnational criminal groups. The United States now provides assistance in a variety of forms—training, equipment, and information—to select units of Mexico's security establishment that are believed to be free of penetration and supportive of the rule of law.[46]

In addition to supporting current Mexican operations against major criminal organizations, the US government is also supporting Mexican efforts at police and judicial reform to ensure that Mexican law enforcement is more efficient in combating the criminal coalitions in a manner consistent with the rule of law. The United States is also supporting education at many levels of the police, judicial system, and in civil society to bolster Mexican democratic forces. For more than five years, the United States has supported partnerships of Mexican and US NGOs to prepare to significantly enhance the educational capabilities of Mexico's schools.

Through major curricula, teacher training, and other techniques, Mexican adolescents will learn about the rule of law and develop the skills to further a culture of lawfulness in their society.[47] This has recently been expanded to police education at the state and federal levels. Now all levels of police—from new recruits to commanders—are beginning to receive rule of law and integrity education.

These efforts expanded in 2008, and the Mexican government has established a multiparty, multisector governmental and nongovernmental formal coalition, including most major sectors—media, business, labor, faith-based and secular, centers of moral authority—to both enhance the security capabilities of the state and to change the culture, so it is more supportive of lawfulness. The United States likewise is encouraging partnerships and programs between US and Mexican governmental and nongovernmental organizations, both against criminality and in support of the rule of law.

But there is no unity of effort or coordination of the democratic anticriminal forces. Parts of the Mexican and the US governments and some in Europe are players. They in turn support some Mexican and US nongovernmental players. Some of the nongovernmental players collaborate with their partners across the border with no governmental involvement, mobilizing the populace and reinforcing reforms, efficiency, and commitment to ensure the Mexican states do not submit to the armed group coalitions. In the face of this lack of unity of effort and coordination, irregular conflict in Mexico will be ongoing.

The Twenty-First-Century Difference

The security paradigm of the twenty-first century, as Rupert Smith proposed in *The Utility of Force*, cannot be understood through the lens of its twentieth-century, state-centric counterpart. Not only has the global structure shifted markedly, this has been accompanied by important changes in the nature of instability, conflict, and war as well. A decade into the twenty-first century, patterns of instability and conflict can be discerned. From those developments emerge several broad dimensions.

Today, there are many more actors—armed groups, states, and other nonstate actors—employing an array of irregular means to achieve their goals. This makes for a far more complex field of engagement. Consider the conflicts taking place in and around Pakistan, Mexico, Nigeria,

Afghanistan, Lebanon, Somalia, and Yemen. The strategies and techniques employed by armed groups and the states that back them in these fights differ markedly from those used in twentieth-century wars.

Facilitating the emergence of many of these new actors is the fact that more than half the world's states are weak, failing, or failed. Their governments lack legitimacy, are often corrupt, and cannot control their territory. Armed groups, which incubate, mature, and become empowered in these weak and failing states pose an array of differing challenges. Some take the form of extremist groups with political agendas, others of criminal enterprises. Yet other weak states are threatened by multiple and diverse armed groups.

These first two developments provide opportunities for decentralized armed groups, other nonstate actors, and states to pursue their objectives at the local, national, regional, and even sometimes at the global level. And they are doing so through new types of coalitions, partnerships, and networks which are capable of challenging the United States and other democracies. The capacity of armed groups to transform and to establish linkages with state and nonstate actors greatly complicates the ability of the security services of states to understand them.

As a result, terrorists and criminal organizations are able to hit targets in Europe, Asia, Africa, and North America. Crime cartels are players in Mexico as well as in Central and South America. Experts predict that cyber attacks or the use of biological, chemical, and even weaponized nuclear materials are on the horizon, expanding the potential geographic and casualty ranges that are in play.

Moreover, there are no front lines to identify and attack in these situations. In this type of irregular warfare, the adversary uses many nontraditional tactics—assassinations and roadside bombs, suicide attacks, bribery, propaganda in the new and old media—to slowly gain power over territory and populations. The theater of conflict includes streets, neighborhoods, villages, websites, schools, and television—settings where local governments are often weak, targets are highly vulnerable, and the effectiveness of conventional military power is diminished or irrelevant.

A New Security Agenda

Adapting to this twenty-first-century security context will be a major challenge for the United States. To do so, it will have to make a paradigm

shift in how it understands security threats, the capabilities needed to protect and defend against these challenges, and how best to organize, recruit, train, and educate to develop those capabilities. This will necessitate refocusing on the most likely irregular conflicts and challenges. Those conflicts are happening today and, for the reasons highlighted above, will persist well into the foreseeable future.

To meet and manage twenty-first-century irregular conflicts, the United States military and civilian security agencies will need to adapt and improve their instruments and capabilities. We are at one of those crossroads in history. Just as horses were sent back to the stables in 1914 and tanks became the new cavalry, a new set of tools and tactics will need to be developed and employed. In today's complex world there is no one solution, no silver bullet. Managing challenges emanating from the irregular conflict environment over the next several decades will require a new US security focus led by military, intelligence, and civilian operators.

What follows is a proposed agenda of five categories of instruments and capabilities the US will require if it is to effectively manage these irregular challenges between now and at least 2025. The good news is, establishing and building up these capabilities will not entail major additional budget commitments. In national security terms they are not big-ticket items, like advanced technology, aircraft carriers, or more troop divisions. The bad news is they are now in short supply or do not exist at all in the US inventory.

Moreover, each of the five categories of capabilities listed below, to be fully matured, will require developing new concepts of operations, requisite doctrine, tools and techniques, personnel, and the necessary authorities.

1. *Selected Army and Marine Corps units will need to be adapted, reoriented, and retrained for irregular conflict as their primary mission*. They must be prepared to support local struggles against armed groups with both kinetic and nonkinetic tools. The answer is not to add more manpower but to make different and better use of the existing forces to execute irregular missions. For example, military skills must be adapted and meshed with civilian skill sets to produce adaptable rule of law and security sector reform—which will help us win the conflict.
2. *To make sense of the new "battlefield"—which usually lacks a front line and often involves civilians as players—US and allied forces need much better intelligence at the local level.* This necessitates development of intelligence units focused on the local level. This is critical to help

distinguish who is part of an armed group, who is assisting them, who is engaging only in political dissent, and who can work effectively locally against the armed group networks. Such intelligence can be acquired if the United States develops new units able to train frontline foreign police, military and security collectors, analysts, and others to operate at the local level to complement formidable national capabilities of the United States and its allies.

3. *Security, Stability, Reconstruction, and Rule of Law/Culture of Lawfulness Teams that are professionalized in greater numbers to manage and/or prevent the outbreak of irregular conflict and to strengthen weak governments and civil society are required*. The goal is to help build governments whose legitimacy is recognized by citizens and to inculcate rule of law principles and understanding in the population. Rather than waiting for weak states to slip into critical conditions, we need to employ the twenty-first-century security equivalents of "wellness programs" to bolster and support them. Repeated full-scale military operations to rescue failing states are too costly in money and human terms for the United States to shoulder. Building a comprehensive capability will require the United States to develop systematic plans, personnel, and resources to act in diverse environments.

4. *Enhanced strategic communication management tools must be developed.* Senior US leaders, national security managers, and local implementers must have the skill sets to understand and manage their words and actions so they resonate with and influence the perceptions and behaviors of foreign audiences, especially at the local level in irregular conflict zones. The goal is ultimately to persuade local leaders and populations to change their behaviors. To do so successfully with effective tools, the US government must understand how the audience perceives the world and US actions; what their attitudes are toward the behavior change the United States is seeking; and how those attitudes have been formed. Words and actions must be gauged to be effective. If not, the goal will likely not be reached. Strategic communication is about managing these perceptions.

5. *New political advisors and mediators are needed to build coalitions in irregular conflict environments.* The United States needs professional, skilled personnel—military and civilian—capable of bringing together coalitions of actors to prevent or prevail in irregular conflicts with

adversarial coalitions. These mediators and coalition facilitators would operate with the authority, skills, and resources needed to work with both senior and local leaders and groups to enhance their effectiveness. Creative US individuals have played extraordinary roles in recent years, but professional programs do not exist in this area to build expertise and continuity or to integrate these activities into operations.

The specific configuration and deployment of these five categories of military and civilian capabilities will be determined by the local political and security context or conflict zone in which the United States is engaged. Three scenarios are envisioned.

The *first* are small advisory missions that are mainly preventative in scope and have as their objective assisting or building local capacity, particularly in fragile democracies. These missions aim to address the origins of weaknesses before they generate violent instability that might spread from local to regional levels. They should receive a high priority. The *second* involves limited US presence "on the ground" such as in Pakistan and Colombia. The *third* are major population-centric security operations against robust, armed groups in war zones where the US military is or was the main security force, as in Afghanistan and Iraq.

In closing, it should also be emphasized that these capabilities, even if developed and deployed, are not a panacea or cure-all for the irregular challenges ahead. As we stated above, in today's complex world there is no one solution, no silver bullet. But, if the United States does not invest in these capabilities now, they will not be available in specific theaters and conflicts where their presence could decrease the costs in lives and treasure and determine the outcome. They are tools that will substantially enhance the United States' ability to manage irregular conflict challenges, providing the means to protect American interests and allies in key regions of the world. SSQ

Notes

1. The article was prepared in 2010 under the auspices of the National Strategy Information Center project, "Adapting America's Security Paradigm and Security Agenda." Details and findings of the project, to include a major report released in March 2010, can be found at www.strategycenter.org. A book published from the project provides the specifics of how instability, conflict, and war in the twenty-first century have changed in significant ways; highlights how those changes challenge the United States and other democracies; and identifies specific capa-

bilities that the United States and its allies need to develop to manage and mitigate the threats emerging from this new environment.

2. Charles Krulak, "Ne Cras: Not like Yesterday," in *The Role of Naval Forces in 21st Century Operations*, eds. Richard Shultz and Robert Pfaltzgraff (Washington: Brassey's, 2000), xi–xii. Also see Krulak, "Operational Maneuver from the Sea," *Joint Force Quarterly* (Spring 1999), 79.

3. Writing just before 9/11, Anthony Lake wished that he and others in the Clinton administration had devoted more attention to what were usually tier II and III concerns in most of the Clinton years. See Anthony Lake, *Six Nightmares: Real Threats in a Dangerous World and How America Can Meet Them* (Boston: Little, Brown and Co., 2000).

4. Rupert Smith, *The Utility of Force: The Art of War in the Modern Age* (New York: Alfred Knopf, 2007), 5.

5. DoDD 3000.07, *Irregular Warfare*, December 2008, 2, www.dtic.mil/whs/directives/corres/pdf/300007p.pdf.

6. The International Peace Research Institute in Oslo (PRIO), in association with the University of Uppsala Data Conflict Program in Sweden, records global armed conflicts annually, dividing them into four categories: interstate, intrastate, extrastate, and internationalized internal conflict. Their database also illustrates the rise in the number of conflicts fought between states and armed groups. According to PRIO, in the 1950s these represented between a third and one half of all conflicts, whereas by the 1990s they accounted for nearly all armed conflict. This trend has continued since 9/11. Uppsala Conflict Data Program charts are available at http://www.prio.no/cwp/ArmedConflict/ and at http:///www.pcr.uu.se. Mikael Eriksson, Peter Wallensteen, and Margareta Sollenberg, "Armed Conflict, 1989–2002," *Journal of Peace Research* 40, no. 5 (2003): 593–607. This study documents that a total of 226 armed conflicts have been recorded for the years 1946–2002. Of these, 116 were active in the period 1989–2002, including 31 in 2002. The data for this study are drawn from the Uppsala Conflict Data Program Armed Conflict webpage at www.prio.no/cwp/ArmedConflict/ and at www.pcr.uu.se. Similar trends were identified by Kalevi J. Holsti and other scholars in the 1990s. See Holsti, *The State, War, and the State of War* (Cambridge, UK: Cambridge University Press, 1996). Also see Zalmay Khalilzad and Ian O. Lesser, eds., *Sources of Conflict in the 21st Century: Regional Futures and U.S. Strategy* (Santa Monica, CA: RAND, 1998), http://www.rand.org/pubs/monograph_reports/MR897.html; Ted R. Gurr, *Peoples versus States: Minorities at Risk in the New Century* (Washington: US Institute of Peace, 2000); Donald L. Horowitz, *Ethnic Groups in Conflict*, 2nd ed. (Berkeley: University of California Press, 2000); Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era* (Stanford, CA: Stanford University Press, 1999); Sudhir Kakar, *Colors of Violence*: *Cultural Identities, Religion and Conflict* (Chicago: University of Chicago Press, 1996).

7. The US Fund for Peace *2009 Failed State Index* ranks 177 states in order of their vulnerability to violent internal conflict and societal dysfunction. A state's overall assessment is based on 12 social, economic, political, and military indicators. The full data set from the *Failed State Index* can be accessed at: http://www.fundforpeace.org/web/index.php?option=com_content&task=view&id=292&Itemid=452. The Brookings Institution's *Index of State Weakness in the Developing World* ranks 141 developing countries according to 20 indicators divided into four categories—economic, political, security, and social welfare. This index ranks 28 states as "critically weak" and another 28 as "weak." A third group of 28 is categorized as "states to watch" because they exhibit "significant weakness in particular areas" and "increased overall fragility." Of the 144 states ranked, 92 are failed, weak, or fragile. See Susan E. Rice and Stewart Patrick, *Index of State Weakness in the Developing World* (Washington: Brookings, 2008), http://www.brookings.edu/~/media/Files/rc/reports/2008/02_weak_states_index/02_weak_states_index.pdf.

8. See Roy Godson and Jose Manuel Vergara, *Democratic Security for the Americas: Intelligence Requirements* (Washington: National Strategy Information Center, 2008). Also see "The Failed State Index," *Foreign Policy* (July/August 2008).

9. Angel Rabasa and John E. Peters, *Ungoverned Territories: Understanding and Reducing Terrorism Risks* (Santa Monica, CA: RAND, 2007). Chapters 12–13 focus specifically on ungoverned territories in the Mesoamerica region. The initial chapters, specifically chapters 1–3, focus on describing the dimensions of ungovernability and what makes these territories conducive for armed groups to establish a presence in them.

10. Different research organizations have established databases on armed groups. For example, the International Institute for Strategic Studies' Armed Conflict Database contains information on the composition, growth, and activities of over 270 armed groups (www.iiss.org). Databases have also been compiled by Jane's Information Group/Sentinel Security Assessments (www.janes.com), Global Security (www.globalsecurity.org), and the Federation of American Scientists' Intelligence Resource Program (www.fas.org/irp).

11. Colleen Cook, *Mexico's Drug Cartels* (Washington: Congressional Research Service [CRS], February 2008); Anna Gilmore, "Pressure Mounts on the Gulf Cartel," *Jane's Intelligence Review* (January 2009); Oscar Becerra, "A to Z of Crime: Mexico's Zetas Expand Operations," *Jane's Intelligence Review* (January 2009); Ioan Grillo, "Mexico's Narco-Insurgency," *Time*, 25 January 2008; George W. Grayson, *Mexico: Narco-Violence and a Failed State?* (Piscataway, NJ: Transaction Publishers, 2009).

12. Cook, *Mexico's Drug Cartels*; Oscar Becerra, "New Traffickers Struggle for Control of Mexican Drug Trade," *Jane's Intelligence Review*, 1 September 2004; Stephen L. Mallory, *Understanding Organized Crime* (Sudbury, MA: Jones & Bartlett Publishers, 2007); Roy Godson, ed., *Menace to Society: Political-Criminal Collaboration around the World* (New Brunswick, NJ: Transaction, 2003).

13. Among the books that chronicle and assess Operation Iraqi Freedom and its immediate aftermath in which these developments transpired are: Michael R. Gordon and Bernard E. Trainor, *Cobra II*: *The Inside Story of the Invasion and Occupation of Iraq* (New York: Pantheon, 2006); John Keegan, *The Iraq War* (New York: Vintage Books, 2005); and Thomas Ricks, *Fiasco: The American Military Adventure in Iraq* (New York: Penguin Press, 2006).

14. Richard Shultz and Andrea Dew, *Insurgents, Terrorists, and Militias: The Warriors of Contemporary Combat* (New York: Columbia University Press, 2006), chap. 7; and Ian F. W. Beckett, *Insurgency in Iraq: A Historical Perspective* (Carlisle, PA: Strategic Studies Institute of the US Army War College, March 2005).

15. Ahmed Hashim, *Insurgency and Counterinsurgency in Iraq* (Ithaca, NY: Cornell University Press, 2006), chap. 3: Shultz and Dew, *Insurgents, Terrorists, and Militias*, chap. 7; Bruce Hoffman, "Insurgency and Counterinsurgency in Iraq," *Studies in Conflict & Terrorism* (March/April 2006).

16. International Crisis Group, *Nigeria: Failed Election, Failing State?* Africa Report no. 126, 30 May 2007, http://www.crisisgroup.org/en/regions/africa/west-africa/nigeria/126-nigeria-failed-elections-failing-state.aspx.

17. Daniel Jordan Smith, *A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria* (Princeton: Princeton University Press, 2007); and Thomas O'Neill, "The Curse of Black Gold: Hope and Betrayal in the Niger Delta," *National Geographic*, February 2006.

18. Rabasa and Peters, *Ungoverned Territories*, chap. 9; and Kenneth Omeje, *High Stakes and Stakeholders: Oil Conflict and Security in Nigeria* (Farnham, UK: Ashgate Publishing, 2006).

19. Stephanie Hanson, "MEND: The Niger Delta's Umbrella Militant Group," backgrounder, Council on Foreign Relations, 2007, http://www.cfr.org/publication/12920; and International

Crisis Group, *The Swamps of Insurgency: Nigeria's Delta Unrest*, August 2006, www.crisisgroup.org/home/index.cfm?id=4310.

20. "Nigeria—The Significance of the Bonga Offshore Oil Platform Attack," *The Oil Drum*, 24 January 2008, www.theoildrum.com/node/4196.

21. "Nigerian Militants Warn of Oil War," *BBC News*, 14 September 2008, http://news.bbc.co.uk/2/hi/africa/7615498.stm.

22. Ana Arana, "How the Street Gangs Took Central America," *Foreign Affairs* 84, no. 3 (May/June 2005); John Sullivan, "Maras Morphing: Revisiting Third Generation Gangs," *Global Crime* (August 2006); and S. C. Boraz and Thomas Bruneau, "Are the Maras Overwhelming Governments in Central America?" *Military Review* (November/December 2006).

23. John Sullivan, "Transnational Gangs: The Impact of Third-Generation Gangs in Central America," *Air & Space Power Journal* (June 2008); and Max G. Manwaring, *Street Gangs: The New Urban Insurgency* (Carlisle, PA: Strategic Studies Institute of the US Army War College, 2005).

24. Shultz and Dew, *Insurgents, Terrorists, and Militias*, chap. 7.

25. F. Gregory Gause III, "Saudi Arabia: Iraq, Iran, the Regional Power Balance, and the Sectarian Question," *Strategic Insights* (March 2007), www.ccc.nps.navy.mil/si/2007/Mar/gauseMar07.pdf.

26. K. Katzman, *Iran's Influence in Iraq* (Washington: Library of Congress, 2007); and Vali Nasr, "When the Shiites Rise," *Foreign Affairs* 85, no. 4 (July/August 2006).

27. Mohammad Hafez, *Suicide Bombers in Iraq* (Washington: US Institute of Peace, 2007); and Assaf Moghadam, *The Globalization of Martyrdom: Al Qaeda, Salafi Jihad, and the Diffusion of Suicide Attacks* (Baltimore: Johns Hopkins University Press, 2008).

28. Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press, 2002); Quintan Wiktorowicz, "Anatomy of the Salafi Movement," *Studies in Conflict & Terrorism* (April–May 2006): 207–39; and Mark Sedgwick, "Al-Qaeda and the Nature of Religious Terrorism," *Terrorism & Political Violence* (October–December 2004), 785–814.

29. Richard H. Shultz, *Global Insurgency and Salafi Jihad Movement* (Boulder, CO: Institute for National Security Studies, 2008); Gabriel Weimann, "How Modern Terrorism Uses the Internet," *US Institute of Peace Special Report* 116 (March 2004); Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington: Potomac Books, 2006); Robert Bunker, *Networks, Terrorism, and Global Insurgency* (London: Taylor & Francis, 2006); and John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in *Terrorism and Counterterrorism: Understanding the New Security Environment, Readings and Interpretations*, eds. Russell Howard and Reid Sawyer (New York: McGraw Hill, 2006), 39–72.

30. Rohan Gunaratna, "Al-Qaedastan: The Terrorist Sanctuary on the Afghan-Pakistan Border," *The Intel File Special Operations Report* (Winter 2008), http://events.fcw.com/events/2008/GLR/downloads/GLR08_T1_GUNARATNA_THE%20TERRORIST%20SANCTUARY%20OF%20THE%20AFGHAN-PAKISTAN%20BORDER.pdf.

31. Thomas Friedman coined the term "super-empowered individual" in his 1999 book *The Lexus and the Olive Tree* (New York: Random House, 2000, expanded edition). Since Friedman introduced the concept, few specialists have sought to expand on its parameters. But, there is the need to do so given the fact that today there are nonstate micro actors, to include individuals, groups, and institutions that have the capacity to impact the security environment by facilitating conflict and instability. They do so without employing their own armed capability. Rather, they have the capability to contribute to internal, regional, and international instability in a number of other indirect ways.

32. Andy Rowell, "U.S. Increases Military Assistance in the Niger Delta," *Oilchange International*, 16 March 2007, http://priceofoil.org/2007/03/16/us-increases-military-assistance-in-niger-delta/.

33. Esther Pan, "Middle East: Syria and Lebanon," backgrounder, Council on Foreign Relations, 18 February 2005, www.cfr.org/publication/7851/; and Robert Rabil, *Embattled Neighbors: Syria, Israel, and Lebanon* (Boulder, CO: Lynne Reinner Press, 2006).

34. Magnus Ranstorp, *Hizb'allah in Lebanon: The Politics of the Western Hostage Crisis* (New York: Macmillan, 1997); Hala Jabar, *Hezbollah: Born with a Vengeance* (New York: Columbia University Press, 1997); Augustus Richard Norton, *Hezbollah: A Short History* (Princeton: Princeton University Press, Studies in Muslim Politics, 2007); Alexus G. Grynkewich, "Welfare as Warfare: How Violent Nonstate Groups Use Social Services to Attack the State," *Studies in Conflict & Terrorism* 31, no. 4 (April 2008): 350–70; Frederic M. Wehrey, "A Clash of Wills: Hizballah's Psychological Campaign against Israel in South Lebanon," *Small Wars & Insurgencies* 13, no. 3 (Autumn 2002): 53–74.

35. Andrew Exum, *Hizballah at War: A Military Assessment* (Washington: Washington Institute for Near East Policy, December 2006).

36. Frank Hoffman, "Hybrid Warfare Challenges, *Joint Force Quarterly* 52, no. 1 (1st Qtr. 2009): 34–39; Gabriel Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," in *New Media and Innovative Technologies*, eds. D. Caspi and T. Azran (Beer Sheva, Israel: Ben-Gurion University Press, 2007).

37. Matthew Levitt, *Hamas: Politics, Charity, and Terrorism in the Service of Jihad* (New Haven: Yale University Press, 2004); and Shaul Mishal and Avraham Sela, *The Palestinian Hamas* (New York: Columbia University Press, 2000).

38. P. R. Kumaraswamy, "India and Israel: Emerging Partnership," *Journal of Strategic Studies* 25, no. 4 (December 2002) 193–200.

39. For a background discussion see Stanley Pimentel, "Mexico's Legacy of Corruption," in Godson, *Menace to Society*.

40. Grayson, *Mexico: Narco-Violence and a Failed State?*; Gilmore, "Pressure Mounts on the Gulf Cartel"; Becerra, "A to Z of Crime"; and Grillo, "Mexico's Narco-Insurgency."

41. *The United States and Mexico: Towards a Strategic Partnership* (Washington: Woodrow Wilson Center, Mexico Institute, 2009).

42. Grayson, *Mexico: Narco-Violence and a Failed State?*; and Cook, "Mexico's Drug Cartels."

43. UN Office of Drugs and Crime, *Drug Trafficking as a Security Threat in West Africa* (November 2008); Liana Sun Wyler and Nicolas Cook, *Illegal Drug Trade in Africa: Trends and US Policy* (Washington: CRS, September 2009; and Marco Vernaschi, "The Cocaine Coast," *Virginia Quarterly Review* (January 2010).

44. Max Manwaring, *A New Dynamic in the Western Hemisphere Security Environment: The Mexican Zetas and Other Private Armies* (Carlisle, PA: Strategic Studies Institute, 2009); *Street Gangs: The New Urban Insurgency* (Carlisle, PA: Strategic Studies Institute, 2005); and John Sullivan, "Transnational Gangs: The Impact of Third-Generation Gangs in Central America," *Air & Space Power Journal* (Spanish edition), July 2008.

45. See Godson and Vergara, *Democratic Security for the Americas*.

46. *The United States and Mexico*; and Clare Ribando Seelke, *Mérida Initiative for Mexico and Central America: Funding and Policy Issues* (Washington: CRS, April 2010).

47. For a background discussion of these efforts see Roy Godson, "Fostering a Culture of Lawfulness on the Mexican–U.S. Border: Evaluation of a Pilot-Based Program," in *Transnational Crime and Public Security: Challenges to Mexico and the United States*, eds. John Bailey and Jorge Chabat (San Diego, CA: Center for U.S.–Mexican Studies at UC San Diego, 2002).

Deciphering Cyberpower

Strategic Purpose in Peace and War

John B. Sheldon

What is the strategic purpose of cyberpower? All too many works on cyberspace and cyberpower are focused on the technical, tactical, and operational aspects of operating in the cyber domain. These are undoubtedly important topics, but very few address the strategic purpose of cyberpower for the ends of policy. Understanding its strategic purpose is important if policy makers, senior commanders, and strategists are to make informed judgments about its use. Cyberpower does indeed have strategic purpose relevant to achieving policy objectives. This strategic purpose revolves around *the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment*.

While it is proper to pay attention to the technological, tactical, and operational implications, challenges, and opportunities of cyberspace, this article concerns itself with its use—"the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power"—for achieving the policy objectives of the nation.[1] Transforming the effects of cyberpower into policy objectives is the art and science of strategy, defined as "managing context for *continuing advantage according to policy*" (emphasis in original).[2] The definition provides the overall strategic impetus for the use of cyberpower. To fully understand the power of cyber, one must acknowledge the character of cyberpower and cyberspace. The linkage between strategic context, strategy, and

The author wishes to thank Derek Reveron, Naval War College; Col Harold J. Arata, USAF, and his exemplary team at the Center for Cyberspace Research; Drs. Harold R. Winton, Richard Muller, James W. Forsyth Jr., Stephen Wright, and Stephen D. Chiabotti at the School of Advanced Air and Space Studies; and Lt Col William E. Young, USAF, currently at Air War College.

John B. Sheldon, PhD, is professor of space and cyberspace strategic studies at the School of Advanced Air and Space Studies and deputy director of the AF Space and Cyber Strategy Center, Maxwell AFB, AL. He also teaches cyber strategy at the AF Institute of Technology's Cyber 200 and Cyber 300 courses at Wright-Patterson AFB, OH. Prior to his current duties, he served in Her Britannic Majesty's Diplomatic Service.

cyberpower is also essential. Ultimately, cyberpower stems from the ability to manipulate the strategic environment, and this requires a theory of cyberpower.

The Character of Cyberspace and Cyberpower

It is worth noting the difference between the terms *cyberspace* and *cyberpower*. Cyberspace is the domain in which cyber operations take place; cyberpower is the sum of strategic effects generated by cyber operations in and from cyberspace. These effects can be felt within cyberspace, as well as the other domains of land, sea, air, and space, and can also be cognitively effective with individual human beings. With this in mind, we turn our attention to some of the main characteristics of cyberspace.

Cyberspace relies on the electromagnetic spectrum (EMS). Cyberspace cannot exist without being able to exploit the naturally existing electromagnetic spectrum. Without the EMS, not only would millions of information and communications technologies (ICT) be unable to communicate with each other, but the ICTs themselves would be unable to function. Integrated circuits and other microelectronic devices depend on electrons to function. Fiber-optic cables are nothing if they are unable to propagate light. Networks of ICTs are also dependent upon the myriad properties of the EMS for their essential connectivity via radio frequencies and microwaves.[3]

Cyberspace requires man-made objects to exist. This makes cyberspace unique when compared to the land, sea, air, and space domains. Without integrated circuit boards, semiconductors and microchips, fiber-optics, and other ICTs, there would be no cyberspace capable of hosting the EMS. Space would still exist if humankind were not able to place satellites in Earth orbit; the sea would still exist if humans had been unable to master the intricacies of buoyancy; and similarly, the air would still exist if the principles of flight had not been discovered. Cyberspace would not exist were it not for the ability of human beings to innovate and manufacture technologies capable of exploiting the various properties of the EMS. Without such technologies the EMS would be nothing more than the "Luminiferous Ether" promulgated by the scientist Albert A. Michelson in the late nineteenth century—in other words, though it can be said to exist, the velocity of the earth's orbit around the sun has no discernable effect on it.[4]

Cyberspace can be constantly replicated. As an entity, there is only one air, one sea, one space, and one land. In contrast, there can be as many cyberspaces as one can possibly generate. In reality, there is only one portion of the air, sea, or land that is important: that portion that is being contested. The air over the United States is pretty much the same as that over Afghanistan. The only difference is that the air over the United States is not contested like the air over Afghanistan (or at least, it is contested in principle if not in practice). The same goes for the oceans. One could set off across the Atlantic tomorrow and have a more or less pleasant passage to Europe on the same ocean that, several thousand miles away off the Horn of Africa, is infested with pirates. With cyberspace, however, there can be many in existence at any one time—some contested, some not. For the most part, nothing is final in cyberspace.[5] With airpower, enemy aircraft can be destroyed, and there the matter ends. In cyberspace, a jihadist website can be purposefully shut down, only for the same jihadists to start a new website within hours on a different server using a different domain name. Similarly, networks can be quickly repaired and reconstituted, thanks to the relatively inexpensive and readily available hardware.[6]

The cost of entry into cyberspace is relatively cheap. The resources and expertise required to enter, exist in, and exploit cyberspace are modest compared to the resources and expertise required for exploiting the land, sea, air, and space. Generating strategic effect in cyberspace does not require a budget of billions, manpower in the thousands, tracts of land, or divisions/fleets/wings/constellations of hardware that cost yet more billions of dollars. Rather, modest financial outlays, a small group of motivated individuals, and access to networked computers that are accessible to a large portion of the world's population can provide entry to the cyber domain.[7] Deep computer expertise is always an advantage but not always necessary. Computer science and programming knowledge need be only modest to generate strategic effect in and from cyberspace. As Col Stephen Korns points out, many cyber "weapons" are now commoditized and can be easily purchased "off the shelf" at affordable prices, such as denial-of-service software that can be downloaded onto a personal computer and deployed against its target.[8] The commoditization of cyber capabilities is evidenced by the cyber attacks that took place against Estonia in April/May 2007 and against Georgia in August 2008, when individuals—the vast majority of whom were not experts in programming or computer science—downloaded readily available software to mount the denial-of-service attacks.[9] This is

not to imply that deep cyber expertise cannot bring about an advantage or that the investment of billions of dollars into a cyber effort will not have a significant strategic return—far from it. Rather, the character of cyberspace is such that the number of actors able to operate in the domain and potentially generate strategic effect is exponential when compared to the land, sea, air, and space domains.

For the time being, the offense rather than the defense is dominant in cyberspace. This is due to a number of reasons. First, network defenses rely on vulnerable protocols and open architectures, and the prevailing network defense philosophy emphasizes threat detection, not fixing vulnerabilities.[10] Second, attacks in cyberspace occur at great speed—for all intents and purposes to a human observer they seem instantaneous—putting defenses under immense pressure, as an attacker has to be successful only once, whereas the defender has to be successful all of the time. Third, and related to the previous reason, range is not an issue in cyberspace as it is in the other domains. Attacks can emerge from literally anywhere in the world.[11] Fourth, attributing attacks is for the most part problematic, thus complicating any possible response.[12] Fifth, and lastly, the overwhelming reliance on cyberspace throughout modern society, not just in the military, presents any attacker with a target-rich environment, again placing great strain on the ability to successfully defend the domain.[13]

Cyberspace consists of four layers, and control of one layer does not mean control of the others. Cyberspace consists of infrastructure, physical, syntactic, and semantic layers. The infrastructure layer consists of the hardware, cabling, satellites, facilities, and so on. The physical layer consists of the myriad properties of the EMS—electrons, photons, frequencies, and so forth—that animate the infrastructure layer.[14] The syntactic layer consists of the formatting of information and the rules that instruct and control information systems that make up cyberspace. The semantic layer consists of information useful and comprehensible to human users and is essentially the cyber-cognitive nexus. Controlling the infrastructure layer of cyberspace does not necessarily translate into control of the physical, syntactic, and semantic layers. Similarly, semantic control does not require infrastructure control, as evidenced by the prevalence of cyber crime today that effectively exploits the semantic layer. While this proposition is generally true, there are exceptions that depend upon what one is trying to do. If one is trying to destroy and disable a network, then attacking the infrastructure layer alone may well be effective. If, on the other hand, one is

trying to spoof an enemy commander into making certain decisions, then control of the infrastructure layer is largely irrelevant, but control of the semantic layer is everything.[15]

Cyberpower is ubiquitous. Land, sea, air, and space power are able to generate strategic effect on each of the other domains, but nothing generates strategic effect in all domains so absolutely and simultaneously as cyberpower.[16] Given the cyber dependencies of the military, economy, and society in a growing number of countries, and given that cyberspace critically enables land, sea, air, and space power—as well as other instruments of power, such as diplomacy, media, and commerce—cyberpower is ubiquitous. Land, sea, air, and space power can return to barracks, ports, airfields, or, in the case of satellites, be tasked on to another target. Cyberpower does not go back to its sender, nor is it expended.

Cyberpower is complementary. Unlike land, sea, and airpower, but in many ways like space power, cyberpower is largely a complementary instrument, especially when used autonomously. It is indirect because the coercive ability of cyberpower is limited and likely to remain so. For example, consider the cyber attack against Estonia in spring 2007. It is often forgotten that the attacks occurred along with violent protests in Estonia and a political warfare campaign allegedly perpetrated by the Russian government against Estonian interests. None of these—the protests, political warfare campaign, Russian threats and diplomatic protests, or the cyber attacks—swayed the Estonian government. This is even more remarkable given that Estonia is widely regarded as one of the most cyber-dependent countries in the world. It can certainly be argued that the cyber attacks were damaging, disruptive, and a nuisance, but they were not coercive.[17] It is even more evident that the cyber attacks during the short conflict between Russia and Georgia in August 2008 were likewise not coercive. Georgia, especially at the time, was not a particularly cyber-dependent country, and the Russian military campaign was relatively swift and decisive in achieving its objectives against the Georgians. The associated cyber attacks—which have never been publicly attributed to the Russian government but seemed to have been impeccably timed to peak just as Russian forces crossed into South Ossetia and Abkhazia—certainly caused major disruption to Georgian Internet services and several means of communication, but it is implausible to suggest that the Russian military campaign would have been in any way less decisive had the cyber attacks not taken place or had failed.[18]

The assertion that cyberpower is a complementary instrument rests, of course, on the little-observed use of meaningful cyberpower over the past few years. The nightmare scenarios of cyberpower used to switch off power grids, disrupt air traffic control, or bring down Wall Street with a few keystrokes, so beloved by Hollywood, have thankfully yet to occur. This may well change at some point in the future, and in that case the assertion should be thoroughly revised. But for this to happen, coercion must be proven. Shutting down a power grid via cyberpower, for example, would undoubtedly have catastrophic consequences, but rather than coercing its victim to concede to an attacker's demands, it may in fact only invite an even more catastrophic response. Similarly, for all the press about the damage caused by the Stuxnet worm in recent months,[19] it has plainly not coerced Iranian leaders to abandon their nuclear program.[20] Until such time that cyberpower might prove its coercive ability, it can be said, at best, that it is a complementary instrument.

Cyberpower can be stealthy. One of cyberpower's attractions for many users is the ability to wield it surreptitiously on a global scale without it being attributed to the perpetrator. Malicious software can be planted in enemy networks without knowledge until the cyber weapon is activated and causes its intended damage. Databases can be raided for classified or proprietary information, and the owners of that information may not be any the wiser as terabits of data are stolen. Similarly, private citizens can go about their innocent lives only to discover that cyber criminals have ruined their credit rating and maxed out their credit cards because of stolen identity. This ability to stealthily use cyberpower, aided by the inherent difficulties of attributing the identity and motivation of most attackers, makes it a very attractive instrument for governments and other actors.[21]

Other theorists might feasibly identify more attributes of cyberpower than described here, but the preceding discussion has identified the most prominent characteristics pertinent to the wider ensuing discussion. Before addressing the strategic purpose of cyberpower, however, it is necessary to briefly describe the strategic context in which it is emerging as an instrument of power and its relationship to the enduring nature of strategy.

The Strategic Context of Cyberpower

Along with land, sea, air, and space power is a strategic tool that can be used either alone or in combination with other instruments of military

and national power. Cyberpower can be used in peace and war because, among its many other attributes, it is stealthy and covert, relatively cheap, and its use both favors the offense and is difficult to attribute to the perpetrator. Of course, these very same attributes render our own networks vulnerable to cyber attack by others. But, with a more robust cyber-security culture and a more realistic understanding of the limits of cyberpower, we should consider that its value as an instrument to manipulate the strategic environment to one's advantage outweighs the risks.

Cyberspace is but the latest collection of technologies in the history of information processing. The printing press, telegraph, telephone, and wireless communication technologies such as radio and television have each revolutionized society, and in turn military affairs, in their own ways.[22] Cyberspace, however, is different from its technological predecessors because it is not just a means of communication but also the predominant form of creating, storing, modifying, and exploiting information.[23] The technological predecessors of cyberspace—with the possible exception of the book—have always been means of exchanging (transmitting and receiving) information; the creation, storage, modification, and exploitation of that information did not occur within those technologies.

Today, information and communication technologies permeate every function and level of the US military, including the Air Force.[24] An ICT can be anything from a personal computer or cell phone to supervisory control and data acquisition (SCADA) devices that monitor the functioning of utilities, infrastructure, facilities, and other complex hardware.[25] Their use is extensive, pervasive, and growing throughout the US military and beyond. Furthermore, most military hardware is now digitized, making most platforms reliant on ICTs for both their internal functioning and for their coordinated use in both peace and war. When ICTs communicate, or network, with each other it can be said that cyberspace exists.[26] Reliance on ICTs is both spreading and deepening, and not just in the military. Throughout the US economy and society, ICTs play a critical role in the everyday functioning of the country, and the same is also true not only of other industrialized developed countries but emerging and developing countries as well.[27]

This expanding, deepening, and increasingly pervasive reliance on cyberspace is part of the mosaic of the shifting geopolitical and economic global environment that provides the strategic context for the use of cyberpower. Admittedly, this strategic context is challenging for policymakers, commanders,

and scholars to comprehend, as fundamental power shifts are still underway and geopolitical alignments are in flux. Safe to say, however, that the United States and its allies, while still the most important fulcrum of power in the international system, are not necessarily the sole focus of international affairs. As Philip Stephens of the *Financial Times* recently pointed out,

> A multipolar world has been long predicted, but has always seemed to be perched safely on the horizon. Now it has rushed quite suddenly into the present . . . The lazy way to describe the new geopolitical landscape is one of a contest between the west and the rest—between western liberal democracies and eastern market economy autocracies. Neat as such divisions may seem, they miss the complexities. None are more determined, for example, than Russia and China to keep India from securing a permanent seat on the UN Security Council. Few are more worried than India by China's military buildup . . . The rising nations prize state power over international rules, sovereignty over multilateralism. The transition to a new order is likely to see more rivalry and competition than co-operation. The facts of interdependence cannot be wished away but they will certainly be tested. It is going to be a bumpy ride.[28]

Compounding these rapid, and at times dramatic, changes is the fact that cyberpower as a strategic tool has diffused widely among all actors—state and nonstate alike. The United States may continue to hold the preponderance of land, sea, air, and space power, and may well do so with cyberpower, but other actors in the strategic environment are also cyber empowered and are often wielding their cyberpower to some effect.[29] With the strategic context summarized, now consider the relationship between strategy and cyberpower.

Strategy and Cyberpower

Cyberpower is technically, tactically, and even operationally distinct from the other instruments of military power, but it is not beyond strategy; nor does it subvert the enduring nature of war that is unchanging throughout history. Yet while the nature of war is unchanging, its character changes all the time along with changes in society, political actors, technology, geopolitics, and the emergence of new exploitable domains such as the sea, air, space, and more recently, cyberspace.[30] A general understanding of strategy, and in particular, an understanding of the strategic meaning of cyberpower, can help senior commanders and policymakers comprehend what is enduring, what is new and unique, and what is important and unimportant in cyberpower.

Cyberpower is subservient to the needs of policy, and strategy is the process of translating those needs into action. Cyber operations take place in cyberspace and generate cyberpower, but they do not serve their own ends; they serve the ends of policy. Strategy is the bridge between policy and the exploitation of the cyber instrument. The notion that cyber operations (along with land, sea, air, and space operations) must serve their own imperatives is a thoroughly astrategic one. For example, the capability may exist through cyber means to shut down the power grids in foreign nations, disable their networks, or read every digital message they transmit and receive, but the needs of policy will often demand that the power be kept on, the networks remain unmolested, and intelligence garnered from passively monitoring enemy e-mail activity not be used. Such restraint may stem from a variety of reasons, ranging from the very limited and nuanced objectives of policy, to restraint based on proportionality, to fear of unknown consequences from certain cyber actions. Additionally, one may not wish to tip one's hand by demonstrating a capability for a short-term goal that may only be used a couple of times at best before the enemy can devise a plausible defense. Ultimately, cyberpower may be able to deliver the required strategic effect, but leaders may want to rely on other forms of military power, or even other instruments of national power, in any given instance.

It is vital that commanders and senior officials develop a greater understanding not only of the strategic purpose of cyberpower but also its relationship to strategy. Education, experimentation, and experience will be essential in comprehending the relationship and in identifying the strategic purpose of cyberpower.

Manipulating the Strategic Environment through Cyberpower

The characteristics and attributes of cyberpower previously discussed are just some that can be ascribed to it but do not ultimately explain to the strategist what makes it a unique instrument. The key strategic attribute of cyberpower is *the ability in peace and war to manipulate the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment*. This strategic utility extends to all the other strategic domains (or, if one prefers, media), given their ubiquitous dependence upon cyberspace. Indeed, the strategic

environment is now something that is comprehended and refracted increasingly through cyber technologies, and as a result, the strategic potential of cyberpower will increase accordingly. Its ability, therefore, to manipulate an adversary's perception of the strategic environment to one's advantage is a real, if not growing, prospect. Such manipulation produces the strategic effect of misdirection and deception that in turn allows other military and national instruments of power to achieve policy objectives directly. Ultimately, this means that successful applications of cyberpower will be those used in support of, and in conjunction with, other military and national instruments of power to allow these instruments greater leverage and prospects of success.

The currency of cyberpower is information that can be disseminated via a variety of means across, in, and to all the other media. The aim of the cyber strategist is to maximize to the greatest extent possible the various tools (or cyber "weapons") that can, among other things, disrupt and sabotage adversary cyber-dependent activities; deny adversary cyber-dependent communications; steal information that is valuable to the adversary; monitor and spy on adversary activities through cyberspace; and deceive cyber-dependent adversaries into making decisions (or *not* making decisions) that are favorable to the perpetrator through the manipulation of adversary information by cyber means. Ultimately, these and a variety of other actions through cyberpower—used autonomously and in conjunction with other instruments of power—provide the strategic potential to complicate adversary decision making, buy time to allow other instruments of national power a greater chance of success by disrupting or deceiving adversary information, and ultimately subvert, deny, steal, and even destroy information vital to the functioning of a group, society, or economy as part of a wider strategy of punishment or coercion in conjunction with other forms of military power.

Employed autonomously, cyberpower is unlikely to emerge as an independent coercive instrument. Yet its capabilities do provide real strategic value, as events of the past several years have demonstrated. The Stuxnet computer worm has disrupted and, as a result, delayed the Iranian nuclear program by sabotaging the computer operating system used to power its centrifuges.[31] The denial-of-service operation against Georgian cyberspace during the Russian invasion of August 2008 contributed greatly to the inability of Georgian elites to communicate with each other and the outside

world during the military campaign, thus retarding their ability to react to events in a timely manner.[32]

China is using cyberspace to conduct extensive espionage operations against political, governmental, industrial, and military targets throughout the West to gain access to critical Western technologies and glean the strategic and economic intentions of its rivals.[33] One US official claims that Chinese intelligence services have essentially stolen enough classified and proprietary information to fill the Library of Congress.[34] Finally, millions of people—to include members of Congress, the government, and the military—are potential victims of various "phishing" scams that attempt to illicitly obtain sensitive user ID and password information to access proprietary databases and spoof messages from individuals in positions of authority and command to sow confusion, create deception, and dissolve trust within networks.[35] All of these activities are of serious consequence but, in and of themselves, are not coercive. The reason is relatively simple: no matter how effective the autonomous use of cyberpower may be, one cannot underestimate the resilience of adversaries nor forget that they will almost always have recourse to the use of physical violence to resist and strike back.[36]

Indeed, the ubiquitous nature of cyberspace—thanks in turn to the ubiquity of ICTs—has critical implications for military command, defined by Martin van Creveld as "a function that has to be exercised, more or less continuously, if the army is to exist and to operate."[37] Because cyberspace shrinks organizational scope and can reach up, down, and across echelons and stovepipes, it offers military commanders the potential for greater control. Yet, as van Creveld effectively points out, to use a communications technology solely for control of every tactical and operational activity is to abrogate effective command and stifle, if not strangle, tactical and operational performance.[38] Present-day cyber-enabled commanders would do well to emulate Helmuth von Moltke and his judicious use of the telegraph during the late nineteenth century rather than Field Marshal Haig's "telephonitis" during the catastrophic Battle of the Somme in the First World War.[39] The ubiquity of cyberspace may well tempt many commanders to interfere at the lowest echelon and reach forward into tactical fights, yet the imperatives for effective command in the information age are the same as they were in the days of the Roman Empire. These imperatives consist of the ability of the commander to grasp the strategic context of the time; bring internal and external coherence to the force

under command; create a design for how the force is to be used; have the moral and intellectual courage to take action; possess nerve in the face of extreme pressure and uncertainty; create a persona to inspire those under command to not only obey orders in the face of mortal danger but to also follow the commander who inspires them; possess a great intellect that is creative, bold, and curious; possess expertise in the practice of arms, without which there is no credibility; and finally, identify those rare individuals who not only possess the capacity to carry out such imperatives but also epitomize them.[40]

Cyberpower in the hands of a commander who is able to exercise all the imperatives of command will be a very powerful tool. As van Creveld convincingly demonstrates, those commanders who shaped their command structure according to the mission to be accomplished, rather than the technology at their disposal, won. Those commanders who became slaves to the technology at their disposal—be it the telegraph, telephone, or wireless radio—have tended to exert control at the lowest echelons, thus strangling initiative and adaptability. Rather than leading their forces, they were cocooned by their favored means of communication.[41] Thus, in the wrong hands cyberpower will likely amplify the pathologies of poor senior commanders, stifle the ability of junior officers and senior noncommissioned officers to lead and adapt, and render the entire structure of command reliant on the durability and survivability of what is, in essence, a collection of fragile and vulnerable communication links.

Profound implications arise out of these assertions. First, future wars against cyber-savvy adversaries will have to be fought using command systems that anticipate having to fight in a degraded, if not denied, cyber environment. In other words, these systems must be structured in such a way that they can survive when information is not only unreliable but also scarce. Second, senior commanders will have to delegate tactical and even operational authority to subordinate commanders and guide them through the use of mission orders that specify the minimum that must be achieved. And third, for a force to succeed in an information-deprived environment, a greater onus on unit cohesion, training, and (especially for commanders) education in the strategic arts becomes imperative.

Cyberspace, as already mentioned, is fragile and vulnerable to myriad methods of attack and disruption ranging from jamming of the EMS to the hacking of software, insertion of malware into operating systems, or denial-of-service attacks. This vulnerability, when taken together with the

ubiquity of cyberspace and the reliance built upon it, means that cyberpower is an offensive instrument that is ideal for manipulating the strategic environment to one's advantage and ultimately disrupting and even denying the ability of an adversary deprived of individuals steeped in the imperatives of command to effectively command its instruments of national power. In future wars in which cyberpower will feature most prominently, victory will favor the side able to effectively command forces deprived of information while at the same time using it to deceive, deny, demoralize, and disrupt enemies to the extent that their ability to comprehend the strategic environment is sufficiently deprived. Threats to cyberspace are myriad, and as earlier described in the strategic context of cyberpower, there are many sources of this threat. Even with better cyber defenses, especially in the United States, the effective use of cyberpower will see networks disrupted and unreliable for effective communications and use. That said, however, sufficient resilience measures should be instituted as quickly as possible to help facilitate offensive cyber operations.[42]

Strategically this means policy makers and commanders who are today used to making decisions and commanding in an information-saturated environment will have to become accustomed to carrying out their function in the face of information scarcity and, thus, uncertainty. Perhaps the most profound implication of all is future leaders will find that enduring traits of command and strategic acumen will be just as, if not more, important as ever before. Cyberpower not only adds a new layer of fog to war but also to peace, and this will apply to all who utilize it. Continuing advantage will likely turn on both the ability of leaders and commanders to think and act strategically *and* having the most resilient cyberspace networks that while degraded may provide the information edge. As David J. Lonsdale states, "A little information power can go a long way,"[43] but only if leaders and commanders have the strategic acumen to properly manipulate it to their advantage. Uncertainty, not certainty, will be the default condition in a world of cyberpower. To help future leaders and commanders cope, work must begin, albeit incrementally, on building a theory of cyberpower.

Toward a Theory of Cyberpower

It would be wrong to suggest that no attempt has been made to craft a theory of cyberpower to date. Greg Rattray has done the field a great service with his excellent book, *Strategic Warfare in Cyberspace*, and Stuart

H. Starr attempted to lay a framework for a theory of cyberpower in a chapter he contributed to the eminently useful collection of essays, *Cyberpower and National Security*.[44] Both works have contributed much to building a theory of cyberpower, yet both also have drawbacks. Rattray's work is arguably the superior of the two and has many strategic "nuggets" to offer the careful reader, however, it also tends to overemphasize the technological and organizational dimensions at the expense of other pertinent dimensions and relies exclusively on the analogy of strategic airpower.[45] Starr, on the other hand, usefully employs Harold Winton's taxonomy of what a theory should look like but then immediately delves into the tactical and technical weeds and fails to relate cyberpower to its political and strategic context.[46]

Under the rubric of the eternal logic of strategy should be a theory of cyberpower that can aid the commander and cyber operator to maximize its usefulness as an instrument of policy. Land, sea, air, and space power all have a canon of military theory that includes Jomini and von Moltke for land power, Mahan and Corbett for sea power, Douhet and Mitchell for airpower, and Dolman and Klein for space power.[47] To this day these works are taught in the respective staff and war colleges of all the services around the world. Likewise, a theory of cyberpower is deemed useful because "it is based on the proposition that before one can intelligently develop and employ [cyberpower], one should understand its essence."[48] Similarly, ADM J. C. Wylie, USN, one of the finest strategic thinkers of the twentieth century, noted,

> Theory serves a useful purpose to the extent that it can collect and organize the experiences and ideas of other men, sort out which of them may have a valid transfer value to a new and different situation, and help the practitioner to enlarge his vision in an orderly, manageable and useful fashion—and then apply it to the reality with which he is faced.[49]

A theory of cyberpower, then, might just be of some practical use. But what is such a theory supposed to do? What should it, in broad terms, look like? Winton provides five criteria for developing military theory that can be applied to cyberpower and which, at the very least, should be addressed in any attempt.

Define the field. This criterion would delineate what cyberspace and cyberpower are and what they are not. Daniel T. Kuehl recently identified at least 14 definitions of cyberspace, revealing that the study of the strategic application of cyberpower is immature.[50] Reaching some kind of con-

sensus on definitions of cyberspace and cyberpower is ultimately important if a plausible theory is to emerge.

Categorize into constituent parts. The next criterion of a theory is to break the field of study down into its constituent parts. Imagine cyberpower as a citrus fruit, cutting it up into slices, examining each, and then putting them back together to remake the whole. This involves identifying the component parts of what constitutes cyberspace—its infrastructure, physical, syntactic, and semantic layers—and the various tools (or weapons) that can be used to generate effects.

Explain. With cyberpower defined and the workings of its constituent parts understood, the next criterion of a theory is to explain how it does what it does. Ultimately, "theory without explanatory power is like salt without savor—it is worthy only of the dung heap." Here a theory must explain how cyberpower achieves its desired effects in the strategic environment, such as disruption, deception, denial, and so forth. Furthermore, a theory must attempt to identify the circumstances in which cyberpower will be most effective.

Connect to other fields. A theory must then be able to connect cyberpower to the wider universe. In what ways does it interact with the other domains? In what ways is cyberpower mitigated by friction, differences in cultures, economics, and so on? Such a description need not be exhaustive but should at least demonstrate the place of cyberpower within the strategic cosmos.

Anticipate. A good theory should be able to identify those aspects of cyberpower that are likely to be timeless long after society and technology change.[51] Anticipation is not the same as prediction (which is impossible), but is possible by identifying the larger influences of cyberpower that are scalable in the future. It should, of course, be noted that a theory of cyberpower will have its limitations. It will never be able to fully reflect reality and all the random and complex variables that occur. It is impossible for theory to capture such complexity, but it can educate the mind to cope with the complexity and act with purpose despite it.[52] Furthermore, elements such as technologies, actors, and the political context change at alarming and rapid rates, and theory cannot be expected to capture such changes, but a good theory will recognize that change is inevitable. The best a theorist of cyberpower can expect is to get the big things right enough.

Conclusion

The technological and tactical story of cyberpower has been an exciting (if not disquieting) one to date. Yet the strategic story has been slow to develop, partly due to the fact that little effort has gone into identifying exactly what it is that cyberpower strategically provides to its employer. Cyberpower does have a strategic purpose, and it can be understood by exploring its character, strategic context, and relationship to strategy. Ultimately cyberpower translates into the ability to manipulate perceptions of the strategic environment, and this task requires a theory of cyberpower. There is much that is eminently debatable about cyberpower that doubtlessly others will take issue with, but the growing community of cyber thinkers must focus on the strategic implications as a matter of urgency lest they lead the unwitting into catastrophe. SSQ

Notes

1. This article uses Daniel T. Kuehl's definition of *cyberspace*: "A global domain within the information environment *whose distinctive and unique character is framed by the use of electronics and* the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." Daniel T. Kuehl, "Cyberspace and Cyberpower," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009), 28.
2. Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (London: Frank Cass, 2005), 6.
3. See David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 179–200; Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, 30; and Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 5, 29.
4. Albert A. Michelson, "The Relative Motion of the Earth and the Luminiferous Ether," *American Journal of Science* 22, nos. 127–32 (July–December 1881): 120–29. See also Gerald Holton, *Thematic Origins of Scientific Thought: Kepler to Einstein* (Cambridge, MA: Harvard University Press, 1973), 261–352. My thanks to Dr. Stephen Chiabotti of the School of Advanced Air and Space Studies, Maxwell AFB, for relating this useful point to me.
5. Libicki, *Conquest in Cyberspace*, 5–6.
6. Ibid., 84–85.
7. See Col Stephen W. Korns, USAF, "Cyber Operations: The New Balance," *Joint Force Quarterly* 54 (3rd Qtr. 2009): 97–98.
8. Ibid., 99–100.
9. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Ecco, 2010), 11–21.
10. For a critique of the lack of robust cyber defenses in the United States, see ibid. 103–49.
11. Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, 255–56.
12. Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009).
13. On US dependence on cyber, see Clarke, *Cyber War*, 170–75.

14. Libicki refers to the infrastructure layer as the physical layer. I have added the EMS physical layer to Libicki's taxonomy. See his *Conquest in Cyberspace*, 8–10.

15. Ibid.

16. David J. Lonsdale makes a similar point in his *Nature of War in the Information Age*, 184–86.

17. Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy* 27, issue 3 (May 2008): 227–47.

18. See Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008–09): 60–76; US Cyber Consequences Unit, *Overview by the US–CCU of the Cyber Campaign against Georgia in August of 2008* (Norwich, VT: US–CCU, August 2009), http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf; Stéphane Lefebvre and Roger N. McDermott, "Intelligence Aspects of the 2008 Conflict Between Russia and Georgia," *Journal of Slavic Military Studies* 22, no. 1 (January 2009): 4–19; and Timothy L. Thomas, "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia," ibid., 31–67.

19. On Stuxnet, see, among others, Paul K. Kerr, John Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (Washington: Congressional Research Service, December 2010); and David Albright, Paul Brannan, and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* (Washington: Institute for Science and International Security, December 2010).

20. See Daniel Dombey, "US fears faster Iran nuclear arms progress," *Financial Times* (London), 29 December 2010.

21. See, among others, Brenner, *Cyberthreats*; and Clarke, *Cyber War*, 197–200.

22. See, for example, Elizabeth C. Hanson, *The Information Revolution and World Politics* (Lanham, MD: Rowman & Littlefield, 2008), 13–45.

23. See Daniel T. Kuehl's definition of cyberspace cited in note 1.

24. On the dissemination of ICTs throughout the military see, among others, John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (2nd Qtr. 1993); 142–44; Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001), 312–14; and the collected essays in David S. Alberts and Daniel S. Papp, eds., *The Information Age: An Anthology on Its Impacts and Consequences*, vol. 1, pt. 1, *The Information and Communication Revolution* (Washington: National Defense University, June 1997).

25. On SCADA, see Robert A. Miller and Irving Lachow, "Strategic Fragility: Infrastructure Protection and National Security in the Information Age," *Defense Horizons* 59, January 2008.

26. Capt David R. Luber, USMC, and Col David H. Wilkinson, USMC, "Defining Cyberspace for Military Operations: A New Battlespace," *Marine Corps Gazette* 93, no. 2 (February 2009): 40–46.

27. On the dissemination of ICTs throughout societies around the world, see Manuel Castells, *Communication Power* (New York: Oxford University Press, 2009), 54–136; Martin Campbell-Kelly and William Aspray, *Computer: History of the Information Machine*, 2nd ed. (Boulder, CO: Westview Press, 2004), 141–279; and Eric G. Swedin and David L. Ferro, *Computers: The Life Story of a Technology* (Baltimore: Johns Hopkins University Press, 2005), 131–49.

28. Philip Stephens, "On the way to a new global balance," *Financial Times* (London), 16 December 2010.

29. See Joseph S. Nye Jr., "The Future of American Power: Dominance and Decline in Perspective," *Foreign Affairs* 89, no. 6 (November/December 2010): 2–12, for a judicious view of America's prospect in a rapidly changing geostrategic context.

30. On the nature and character of war and cyberpower, see Lonsdale, *Nature of War in the Information Age*, 19–48; and Lonsdale, "Clausewitz and Information Warfare," in *Clausewitz in the Twenty-First Century*, eds. Hew Strachan and Andreas Herberg-Rothe (Oxford: Oxford University Press, 2007), 231–50.

31. Daniel Dombey, "US says cyberworm aided effort against Iran," *Financial Times* (London), 10 December 2010.

32. Korns and Kastenberg, "Georgia's Cyber Left Hook," 60.

33. Northrop Grumman, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, prepared for the US–China Economic and Security Review Commission (McLean, VA: Northrop Grumman, October 2009), http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

34. Clarke, *Cyber War*, 58–59.

35. On "social engineering" methods, such as "spear-phishing," see Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly, 2010), 146–50.

36. A point eloquently raised by Lonsdale, *Nature of War in the Information Age*, 166.

37. Martin van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985), 5.

38. Ibid., 261–75.

39. On Von Moltke's style of command, see ibid., 103–47. See also Daniel Hughes, ed., *Moltke on the Art of War: Selected Writings* (Novato, CA: Presidio Press, 1995); Geoffrey Wawro, *The Austro-Prussian War: Austria's War with Prussia and Italy in 1866* (Cambridge, UK: Cambridge University Press, 1996); and Wawro, *The Franco-Prussian War: The German Conquest of France in 1870–1871* (Cambridge: Cambridge University Press, 2003). On Haig's style of command, see Van Creveld, *Command in War*, 155–68. See also Paddy Griffith, *The Great War on the Western Front: A Short History* (Barnsley, UK: Pen & Sword Military, 2008), 43–55; and David Stevenson, *1914–1918: The History of the First World War* (London: Allen Lane, 2004), 168–71.

40. Lt Col Christopher Smith, Australian Army, *Network Centric Warfare, Command, and the Nature of War*, Study Paper no. 318 (Canberra: Land Warfare Studies Centre, February 2010), 49–56.

41. Van Creveld, *Command in War*, 261-75.

42. There are various views, and a lively debate, regarding cyber defense in the United States. See, among others, Clarke, *Cyber War*, 151–78; Edward Skoudis, "Information Security Issues in Cyberspace," and John A. McCarthy, Chris Burrow, Maeve Dion, and Olivia Pacheco, "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts," both in *Cyberpower and National Security*, 171–205 and 543–56, respectively; Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington: CSIS, December 2008); and *Cyberspace Policy Review: Assuring a Trusted and Resilient Informational and Communications Infrastructure* (Washington: The White House, April 2009).

43. Lonsdale, *Nature of War in the Information Age*, 193.

44. Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, 43–88.

45. See Rattray's use of faulty strategic analogies in *Strategic Warfare in Cyberspace*, especially his chapters on "Development of Strategic Airpower, 1919–1945: Challenges, Execution, and Lessons," (pp. 235–308) and "The United States and Strategic Information Warfare, 1991–1999: Confronting the Emergence of another Form of Warfare," (pp. 309–459).

46. Starr at least provides a starting point, and for that we are in his debt. Starr, "Toward a Preliminary Theory of Cyberpower."

47. See Baron Antoine Henri de Jomini, *The Art of War* (1838; London: Greenhill Books, 1996); Hughes, *Moltke on the Art of War*; Alfred Thayer Mahan, *The Influence of Sea Power upon History, 1660–1783* (1890; Boston: Little, Brown & Co., 1918); Julian S. Corbett, *Some Principles of Maritime Strategy* (1911; Annapolis, MD: Naval Institute Press, 1988); Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1921; Washington: Office of Air Force History, 1983); William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military* (1925; Port Washington, NY: Kennikat Press, 1971); Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (London: Frank Cass, 2002); and John J. Klein, *Space Warfare: Strategy, Principles and Policy* (Abingdon, UK: Routledge, 2006).

48. Harold R. Winton, "On the Nature of Military Theory," in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles Lutes et al. (Washington: NDU Press, 2011), 19–35

49. J. C. Wylie, *Military Strategy: A General Theory of Power Control* (1967; Annapolis, MD: Naval Institute Press, 1989), 31.

50. Kuehl, "From Cyberspace to Cyberpower," 26–27.

51. Winton, "On the Nature of Military Theory," 2–5.

52. See Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 141.

Interagency Task Forces

The Right Tools for the Job

Robert S. Pope, Lieutenant Colonel, USAF

The US government (USG) conducts a host of operations abroad. Some are responses to crises, such as natural disasters, man-made humanitarian emergencies, or an attack on a friendly foreign country. Others are deliberately planned, such as preemptive military strikes or complex postconflict reconstruction and stabilization operations. Still other operations address such long-term issues as countering narcotics trafficking or global terrorism.

In complex operations requiring participants from more than one US agency, coordinated planning and execution at the operational level often is lacking. This leads to redundancies, gaps, friction, and frustration. Several examples herein of US operations abroad highlight both successes and shortcomings. This analysis discusses four organizational reform models and recommends the interagency task force (IATF) as the preferred structure.

Expertise for these many different missions is spread across several executive-branch agencies. The US Agency for International Development's Office of Foreign Disaster Assistance (USAID/OFDA) responds to disasters like the 2004 Asian tsunami and the 2010 earthquake in Haiti. The military conducts offensive and defensive operations, such as coming to the aid of Kuwait and Saudi Arabia after Iraq's 1990 invasion of Kuwait or removing Saddam Hussein from power in the 2003 US invasion of Iraq. The State Department's (DoS) office of the Coordinator of Reconstruction and Stabilization (S/CRS) has been assigned the lead role in postconflict reconstruction and stabilization operations. The DoS Bureau for International Narcotics and Law Enforcement Affairs, together with US law enforcement agencies, most operating under the Department of Homeland Security (DHS), have the leading role in counternarcotics operations abroad.

Lt Col Robert S. Pope is chief of the South Asia branch, USCENTCOM security cooperation division. Previously, he was an international security program fellow at Harvard's Belfer Center for Science and International Affairs, where he conducted much of the research for this article. He holds a PhD in physics and an MS in nuclear weapons effects physics from the Air Force Institute of Technology and an MMOAS from the Air Command and Staff College.

While the United States often has an agency or office with a leading role in a particular mission area abroad, that agency usually cannot accomplish the mission alone. For example, the US responses to the 2004 Asian tsunami and 2010 earthquake in Haiti required substantial contributions from the military and the State Department as well as the OFDA. Current operations in Afghanistan combine military counterinsurgency (COIN) and counterterrorism (CT) operations with the reconstruction and stabilization efforts of a number of agencies, including the State Department, the USAID, the Department of Agriculture, the Department of the Treasury, and the US Geological Survey.[1] Counternarcotics operations outside the United States require assistance from the military and the intelligence community as well as law enforcement and the DoS.

Past and Current Organizational Structures

Before proposing organizational reforms, it is worthwhile to examine the structures used in several past and current US operations abroad to see how these either facilitated or militated against mission success. Four cases are discussed: (1) the Vietnam War, (2) joint interagency task forces (JIATF) for counternarcotics and rule-of-law development, (3) the US response to the 2004 Asian tsunami, and (4) Operation Enduring Freedom in Afghanistan. These examples cover a range of missions, including COIN, counternarcotics, CT, development assistance, reconstruction and stabilization, and natural disaster response.

Vietnam (1964–73)—Counterinsurgency with Reconstruction and Stabilization

Initially, US involvement in Vietnam occurred entirely within individual agency (as well as individual military service) "stovepipes." The military focused first on providing advisors and training to the South Vietnamese military and later on direct military operations. Meanwhile, US civilian agencies—including the State Department, Central Intelligence Agency (CIA), USAID, Department of Agriculture, and US Information Service—all separately pursued their various agendas, which grew to include many programs that would today be called reconstruction and stabilization, as well as COIN activities, then termed "pacification." Each agency operated independently in Washington, in Saigon, and at the provincial level throughout South Vietnam. Though the US ambassador in Saigon was

nominally in charge of the civilian agencies operating in South Vietnam, he was not able to effectively supervise and coordinate all the activities that were underway with separate agency budgets, lines of authority, and divergent institutional cultures. The commander of the US Military Assistance Command, Vietnam (MACV) met regularly with the ambassador, but coordination between the military and civilian efforts was frequently lacking, and neither the MACV commander nor the ambassador had full authority over US efforts in the country.[2]

As US involvement expanded, programs grew in size and complexity, and the initially poor interagency coordination worsened further. In response, the president, secretary of defense, and joint chiefs decided that unity of command was required, so in 1967 the USG created the office of Civil Operations and Revolutionary (later "Rural") Development Support (CORDS).[3] Civil development efforts previously supervised by the US Embassy in Saigon were integrated under MACV, placing both military operations and civilian development activities under the MACV commander, who was under the overall authority of the US ambassador to Vietnam (though in practice the MACV commander reported to the military's US Pacific Command [PACOM], and disputes with the embassy were often elevated to Washington, diminishing the ambassador's de facto authority over MACV).[4] The civilian director of the CORDS held ambassadorial rank equivalent to a four-star general and exercised control over all interagency assets involved in the counterinsurgency effort. In a significant organizational innovation, the civilian CORDS director was dual-hatted as the MACV deputy to the commander for the CORDS, number three in the military chain of command in Vietnam, behind the MACV commander and the military deputy (see fig. 1).[5]

This construct represents the first time a US ambassador ever worked in the chain of command under a general officer, and it not only brought together the civilian COIN operations under a single leader, but it also integrated the civilian and military COIN efforts. Additionally, because of the CORDS director's position in the military chain of command, it provided the civilian counterinsurgency leader with regular access to the military commander and, therefore, to military personnel, logistics, equipment, and funding. The CORDS structure, from the headquarters down through the provinces and hamlets, was an integrated civil-military organization.[6] Richard Stewart, chief historian of the US Army Center for Military History, described the integration:

> Military personnel were . . . put in charge of civilians [and] civilians were . . . put in charge of military personnel to create a truly mixed, interagency team based on skills and abilities, not agency loyalty. . . . When a senior civilian was assigned to a key . . . position, almost invariably he had a military assistant reporting to him and the reverse was true when a military officer was in the principal slot. This blending of military and civilian authority included the use of the power of personnel evaluation or rating authority.[7]

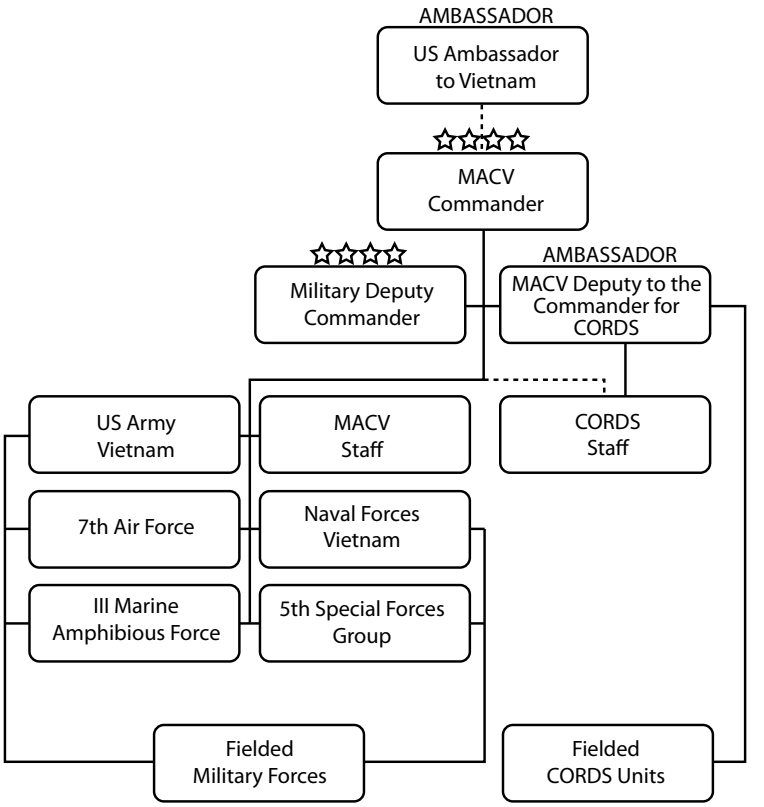

Figure 1. MACV-CORDS organizational structure

While the creation of the integrated civil-military COIN organization vastly improved interagency unity of effort, developing and maintaining the organization faced significant bureaucratic hurdles. The military was generally supportive of the CORDS construct, but civilian agencies were less so.[8] Stewart points to severe bureaucratic shortfalls:

> Presidential leadership proved vital in overcoming the single greatest obstacle to mission success—the reluctance of Washington officials and senior leaders in the field to relinquish control over field operations. The State Department . . . resisted the idea that any of its development or pacification assets should fall under a mili-

> tary chain of command, even one headed by a civilian. Even after several broad hints from the [Johnson] administration, a presidential intervention was needed to change their minds.[9]

Once the CORDS was established, its director had to continually fight Washington-based bureaucratic attempts to reduce its funding, shrink its structure, limit its scope, and keep additional programs from coming under its control.[10] This bureaucratic resistance to formal interagency command structures is probably a primary reason the USG has not used more structures like the CORDS in the decades after Vietnam. While the CORDS produced unity of effort through unity of command and solved the problem of resource asymmetries between military and civilian agencies by providing the civilian agencies with access to military resources, the civilian agencies were never comfortable with the arrangement.[11]

Joint Interagency Task Forces

The Department of Defense (DoD) has attempted to improve interagency unity of effort at the operational level through the creation of joint interagency task forces, which bring together several federal agencies to accomplish an operational-level mission. The US Joint Forces Command (JFCOM), the combatant command charged with military-wide joint doctrine, transformation, and organizational standardization, defines a JIATF as "an interagency organization under a single military director that coordinates counterdrug operations at the operational and tactical level."[12]

The JIATF is "not fully developed in joint doctrine."[13] Indeed, current US joint military doctrine mentions JIATFs in only three publications: Joint Publication (JP) 3-07.4, *Joint Counterdrug Operations*; JP 3-05.1, *Joint Special Operations Task Force Operations*; and JP 3-40, *Combating Weapons of Mass Destruction* (WMD).[14] Thus, while JFCOM's definition limits the JIATF construct to the counternarcotics mission, the concept is at least mentioned in doctrine dealing with special operations and counter–WMD missions.[15]

The JIATF not only receives mere brief mention in military doctrine, but also the construct is neither codified in executive order nor legislation. It derives its authority through a memorandum of agreement signed by the head of each participating agency or department.[16] A JFCOM white paper notes that while agencies subordinate some of their assets under another agency's leadership in a JIATF, these JIATFs do not have true unity of command because "the different agencies still retain many of their

authorities, responsibilities, and prerogatives."[17] However, many of the participating agency and department field-level headquarters are collocated in the JIATF integrated staff structure, enabling the organization to cut across traditional agency stovepipes and facilitate rapid, integrated action.[18]

Two long-standing JIATFs stand out: JIATF-West (JIATF-W) under US PACOM and JIATF-South (JIATF-S) under US Southern Command (SOUTHCOM).[19] Each dates from 1989 and is focused on the counternarcotics mission.[20] In a departure from the JFCOM definition, these two JIATFs are led not by military officers but by Coast Guard rear admirals, who fall under the DHS rather than the DoD.

JIATF-W is PACOM's executive agent for DoD support to counternarcotics initiatives in the PACOM area of responsibility (AOR). It provides interagency intelligence fusion, supports US law enforcement, and develops partner-nation counternarcotics capabilities in the AOR with the goal of detecting, disrupting, and dismantling narcotics-related transnational threats in the region. Initially established in California in 1989 as Joint Task Force 5, in 1994 it was renamed and granted additional interagency authorities and in 2004 was collocated with PACOM headquarters in Hawaii. JIATF-W consists of "approximately 82 uniformed and civilian members of all five military services as well as representatives from the national intelligence community and US federal law enforcement agencies," including the Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), and Immigration and Customs Enforcement (ICE).[21]

JIATF-W has used its interagency mix of capabilities to achieve counternarcotics goals in the region by deploying intelligence analysts to US embassies in the PACOM AOR supporting US law enforcement agencies; constructing interagency intelligence fusion centers for partner nations in the region; constructing infrastructure, such as border patrol stations and customs checkpoints in partner nations; and conducting counternarcotics training for partner-nation militaries and law enforcement agencies.[22]

JIATF-S in Key West, Florida, was created in 1999 by consolidating two other counternarcotics task forces which the DoD had established in 1989.[23] The mission of JIATF-S is to detect, monitor, and consign suspected narcotics trafficking targets to appropriate law enforcement agencies, promote regional security cooperation, and coordinate US country-team and partner-nation counternarcotics initiatives.[24] Because the Posse Comitatus Act places limits on the use of the US military in federal law enforcement, military personnel and assets in JIATF-S can detect and

monitor counternarcotics targets, but enforcement actions must be executed by law enforcement agencies. Since these law enforcement agencies are part of the JIATF, the transition from military monitoring to law enforcement action "happens with little or no disruption."[25]

JIATF-S has an integrated interagency structure, including a USCG rear admiral as its director, an officer from Customs and Border Protection (CBP) as vice director, a senior Foreign Service officer (FSO) as the director's foreign policy advisor (FPA), and participants from all US military services, the USCG, CBP, DEA, FBI, ICE, and elements of the US intelligence community, including the CIA, National Security Agency (NSA), and National Geospatial Intelligence Agency (NGIA). Interagency leadership continues through the lower levels of the organization as well; the directors for intelligence and operations are both military officers, the deputy for intelligence is from the DEA, and the deputy for operations is from CBP.[26] This integrated structure includes an important integrating element—all personnel assigned to JIATF-S, regardless of their parent agency, are evaluated by their bosses on the task force rather than someone from their parent agency, giving JIATF-S the all-important ability to reward personnel for their job at the task force rather than for loyalty to their agency or department.[27]

JIATF-S is a multinational organization, with participants from countries inside and outside the SOUTHCOM AOR working together, both at the headquarters and in combined force packages across the region. France, the Netherlands, and the United Kingdom (all of which govern territories in the AOR) provide ships, aircraft, and liaison officers to the task force, and the commander of the Netherlands Forces Caribbean also commands a subordinate task group. There are liaison personnel from six different AOR nations plus Mexico. This robust liaison program not only facilitates operational cooperation, it also improves information sharing across the region.[28] The JIATF-S organizational structure is shown in figure 2.

Some observers have concluded that JIATF-S is the benchmark interagency organization to emulate. Dr. John Fishel, who has written extensively on civil-military relations, stated that this model is an appropriate organizational construct "to coordinate the activity of many interagency players."[29] LCDR Tom Stuhlreyer, USCG, asserts that JIATF-S is effective and makes best use of limited US resources across the interagency. He notes that narcotics seizure records were being broken at a time when fewer US military assets were available due to high operational require-

ments in the global war on terror, demonstrating "the efficacy and force-multiplying aspect of the joint, interagency, and multi-national approach to operations at JIATF-South."[30] The Government Accountability Office (GAO) credits SOUTHCOM with more success than other combatant commands in its interagency collaboration, in part due to the effect of the JIATF-S organization.[31]

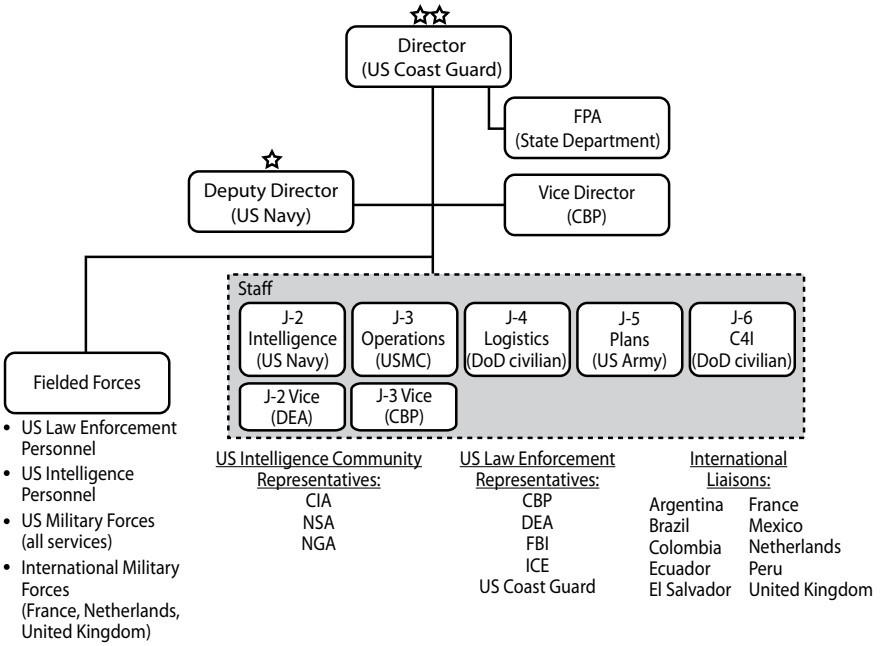

Figure 2. JIATF-S organizational structure

According to Fishel, "The real reason JIATF-S works is that it is structurally an organization that has unity of command. The director is a commander with the authority to hire and fire, as well as to task, organize, and direct actions."[32] However, because JIATFs are not codified in executive order or legislation, the authority remains largely voluntary. Stuhlreyer characterizes the JIATF as an interagency "coalition of the willing" and notes that, while assigned military personnel are subject to normal military order and discipline, the interagency partners "are only obligated to remain invested in JIATF-South as long as the command assists them in achieving individual interagency goals."[33]

Asian Tsunami (2004–05)—Natural Disaster Response

Media reporting on a disaster or humanitarian crisis tends to focus on the military portion of the response, despite the USAID Office of Foreign Disaster Assistance as the lead US agency. The military is frequently the

first and most visible responder with vastly more personnel and equipment than any other US agency.

The response to the 26 December 2004 Asian tsunami provides a good example of a semi-coordinated US interagency response to a humanitarian crisis. The tsunami stretched across South Asia and the coast of Africa and required "the largest humanitarian relief and recovery operation the world has ever seen in the wake of a natural disaster."[34] The US response began within hours of the tsunami. Because the USG lacked a coherent, formalized, interagency approach, the USAID, the DoS, the military, and other federal agencies each began responding individually, using their own procedures.[35]

PACOM led the military response to the disaster and quickly put its joint operations center (JOC) on 24/7 operations. It established a joint task force called Combined Support Force-536 (CSF-536) to conduct military humanitarian response operations. While "Combined" in a unit designation generally refers to a coalition military operation, CSF-536 never exercised operational control over non-US military forces responding to the disaster. Still, much of the international military effort relied on the robust command, control, and communications capabilities provided by the American force. CSF-536 in turn established subordinate combined support groups (CSG) for each country in which the United States responded with significant military forces, and each CSG supported the US ambassador and interagency country team in that country. At the peak of the operation, over 17,000 US military personnel participated.[36]

Because many disasters substantially disrupt local transportation and communication infrastructure, one of the most urgent tasks of the relief effort is providing logistics, transportation, and communication. The CSGs executed search and rescue operations, transported and distributed relief supplies, provided emergency transportation, and contributed to the overall assessment of the disaster. As logistics and transportation infrastructures begin to recover and local government, nongovernmental organizations (NGO), and other responding nonmilitary agencies reach sufficient capability, the military requirement may end relatively early in the response, while other agencies may be engaged for many months or even years.[37]

The USAID also responded quickly to the tsunami. Its OFDA sent disaster assistance response teams (DART) to the affected countries, together with culturally proficient experts to act as liaisons with the host government and local population. The first mission of the DARTs was to

assess the impact of the disaster so relief assistance could be tailored to each country's needs and to the ability of the local infrastructure to receive the aid. Because of the vast size of the affected area, the OFDA provided some training to US military special operations forces and Marine units so they could augment the DARTs. Additionally, OFDA sent a two-man team to PACOM to act as a liaison between PACOM, OFDA headquarters in Washington, and the DART teams in the field.[38]

In each affected country, the US ambassador acted as the overall coordinator of US efforts in that country. The embassies for many of the affected countries had a disaster contingency plan in place, which gave the State Department a starting point for its response. When the tsunami occurred, the embassies developed disaster relief coordination mechanisms with the host government, other diplomatic missions in the country, local NGO representatives, and the US military. They also established status of forces agreements with the local governments, facilitated information flow between the United States and the host nation, and smoothed the flow of relief supplies through customs. In each country, the embassy played a leading role in tailoring the US response, both in terms of the need and the method in which local governments would accept foreign assistance.[39]

To coordinate interagency policy efforts in Washington, the DoS, USAID, and PACOM formed an ad hoc cooperative arrangement. At the regional level, PACOM attempted to provide interagency coordination by establishing a joint interagency coordination group (JIACG) specifically for the disaster response and separate from its standing JIACG.[40] The two-person liaison team sent by the OFDA to PACOM initially worked in this disaster response JIACG but quickly moved to the PACOM JOC, where it was in a much better position to provide situational awareness to the military and serve in a liaison role with Washington and the OFDA teams in the field.

The disaster response JIACG experiment was unsuccessful; the emergency relief phase was largely over before the new JIACG could get organized. However, the OFDA liaison team was very successful in fostering a high degree of mutual confidence among the US interagency participants and thus led to extensive interagency cooperation in the response operations.[41] The interagency organizational structure for the response to this natural disaster is shown in figure 3.

The US response is generally considered a success. The interagency coordination process worked well at the country level in the various embassies,

the regional military response was effective, and USAID's OFDA played its key role, though coordination of these efforts across the region was ad hoc.

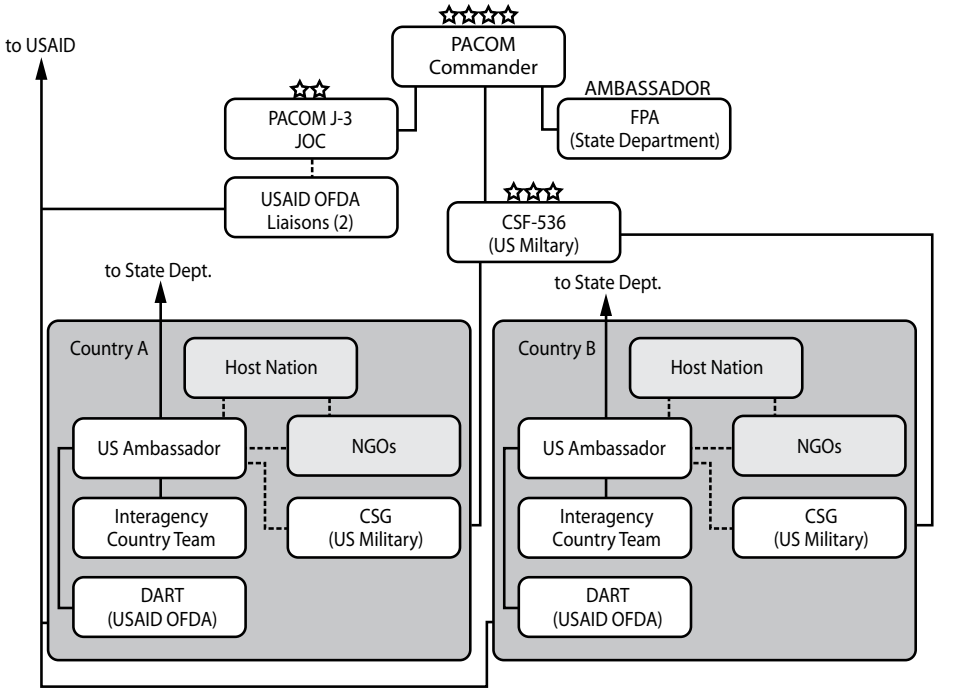

Figure 3. Interagency organization for US response to 2004 Asian tsunami

For single-country disasters this may be good enough, but disasters which affect several countries could be better addressed with a regionally coordinated response. While there is no formal interagency doctrine, process, or organization above the embassy level for US disaster response operations, PACOM's long experience of humanitarian relief planning, exercises, and operations—many times in concert with local partner countries and other US agencies—provided a starting point for the ad hoc regional interagency response to the disaster.[42]

Afghanistan (2001–Present)—Counterinsurgency and Counterterrorism

More than nine years of US operations in Afghanistan have provided the opportunity for a steady evolution of thinking about the need for more-effective, formal coordination of the civil-military COIN campaign. As Operation Enduring Freedom commenced in October 2001, initial coordination was only between the military and the intelligence community (primarily the CIA) for the rapid planning and execution of operations

against al-Qaeda and the Taliban-led government of Afghanistan with minimum use of US forces. Even after the Taliban regime was toppled and large numbers of US forces reached Afghanistan, poor coordination remained between the military, development, and diplomatic communities.

Once the United States reestablished an embassy in Kabul in late 2002, an opportunity for increased civil-military coordination and unity of effort was largely wasted, while the embassy pursued developmental efforts and the reestablishment of the government of Afghanistan. The US military, under LTG Dan McNeill and LTG John Vines, focused on the CT mission. General Vines was emphatic that the military mission was CT and not COIN or nation building, going so far as to prohibit those under his command from using the word *counterinsurgency* to describe their efforts.[43]

US civil-military coordination in Afghanistan greatly improved in 2003–05 under the next US team, Amb. Zalmay Khalilzad and LTG David Barno. General Barno believed in the importance of civil-military coordination to achieving US goals in Afghanistan, so he moved his living quarters to the US Embassy compound in Kabul, established an office next to Khalilzad's, and attended daily embassy country team meetings. Barno also provided the ambassador with five military planners to work with embassy personnel to form an embassy interagency planning group and produce a coordinated US strategy for Afghanistan. The resulting civil-military strategy shifted the US focus from CT to COIN and nation building, created two regional headquarters to direct all coalition actions in each region, and successfully conducted elections, reduced violence, and began reconstruction.[44]

The Khalilzad/Barno civil-military coordination was personality driven and was neither formalized nor directed by either legislation or executive order. In 2005, when Amb. Ronald Neumann and LTG Karl Eikenberry replaced Khalilzad and Barno, civil-military cooperation effectively ended. General Eikenberry returned the military's focus to CT kill-or-capture operations, which led to an increasing number of civilian casualties and consequently a steep decline in Afghan popular support for the United States.[45] Political scientist and Afghanistan expert Seth Jones concluded that this "effectively shatter[ed] the military-civilian coordination Khalilzad and Barno had painstakingly fashioned during their tenure together,"[46] and Senator John McCain said that "Between late 2003 and early 2004, we were moving on the right path in Afghanistan, [but] . . . rather than building on these gains . . . we squandered them. . . . Our integrated civil-

military command structure was disassembled and replaced by a balkanized and dysfunctional arrangement."[47]

In 2007, Amb. William Wood and GEN Dan McNeill replaced Neumann and Eikenberry. GEN David McKiernan replaced McNeill in 2008. During this period, civil-military relations continued largely as they had under Neumann and Eikenberry, with the military primarily focused on kinetic counterterrorism operations and training the Afghan National Army, while civilian agencies worked independently on diplomatic and developmental goals. In early 2009, late in General McKiernan's tour, the United States began moving once again toward more civil-military coordination with the creation of an executive working group (EWG), which each month brought together the in-country principals from the DoS, USAID, and the military to discuss civilian and military plans and operations and synchronize interagency efforts. The high-level EWG was supported by a working-level interagency staff called the Integrated Civilian Military Action Group, staffed by State Department personnel from S/CRS, USAID personnel, and US military personnel from the Regional Command East and the International Security Assistance Force (ISAF).[48]

Many have been critical of the ad hoc nature of US civil-military coordination in Afghanistan. In April 2008 the House Armed Services Committee reported that "rather than depending exclusively on personalities for success, the right interagency structures and processes need to be in place and working."[49] A former senior US military commander in Afghanistan identified the most serious challenge in Afghanistan in 2009 as "not the Taliban . . . not governance . . . not security. . . . It's the utter failure in the unity of effort department."[50] In April of that year, Secretary of Defense Robert Gates expressed his lack of satisfaction with McKiernan's civil-military coordination efforts, saying the NATO ISAF commander needed to focus on "cooperation between civil and military efforts."[51]

The US leadership in Afghanistan changed again in 2009, with retired lieutenant general Karl Eikenberry becoming ambassador on 29 April and GEN Stanley McChrystal becoming the NATO ISAF and US Forces-Afghanistan (USFOR-A) commander on 15 June.[52] Under direction from Washington, the new team quickly set out to develop an integrated civil-military plan. They assembled a planning team led by planners from the S/CRS and including other US civilian agencies as well as the US military from both USFOR-A and ISAF, and on 10 August 2009 released the

Integrated Civil-Military Campaign Plan for Afghanistan over both of their signatures.[53]

The new plan created a coordinated civil-military decision-making structure at all levels in Afghanistan. At the national level in Kabul, the United States established several interagency groups. The principals group (the ambassador and the commanding general of ISAF and USFOR-A) has responsibility for final coordination and decision making. The EWG (with interagency members from the US Embassy, USFOR-A, and US forces from ISAF) includes a deputies-level body to make policy and decisions. Several mission areas in the campaign plan have national-level working groups, which monitor and assess progress on each mission area in the plan. The political-military section of the embassy provides planning and assessment support for the EWG and national-level working groups. In addition, the civilians at the embassy were reorganized along functional, rather than agency, lines.[54]

In the field, the United States created civilian lead positions at the two regional commands, at each subregional US brigade task force, and for each province. These civilian leads coordinate the activities of all US civilians in Afghanistan at their level and subordinate levels who are operating under the ambassador's authority and also serve as the civilian counterpart to the military commander at that organizational level. This dual role as the leader of US interagency civilians and counterpart to the US military commander is intended to produce civil-military unity of effort at each level. In addition, each region has established an organization, called the regional integrated team, composed of the regional command commander, the US Special Operations Forces commander for that region, the civilian lead, and representatives from US agencies operating in the region. Each regional command also has a civil-military fusion cell, which is responsible for maintaining a common operating picture of the region. Similar civil-military entities operate at the subregional, provincial, and district levels. While these civil-military structures are currently US–only, the campaign plan indicates they could be expanded to include non-US military forces and civilian participants.[55] The US organizational structure in Afghanistan is shown in figure 4.

While this parallel civilian-military organizational structure (plus the three recent CJIATFs focused on counternarcotics and rule of law) is the closest civil-military coordination the United States has produced in nine years of operations in Afghanistan, it still falls short of the truly integrated CORDS

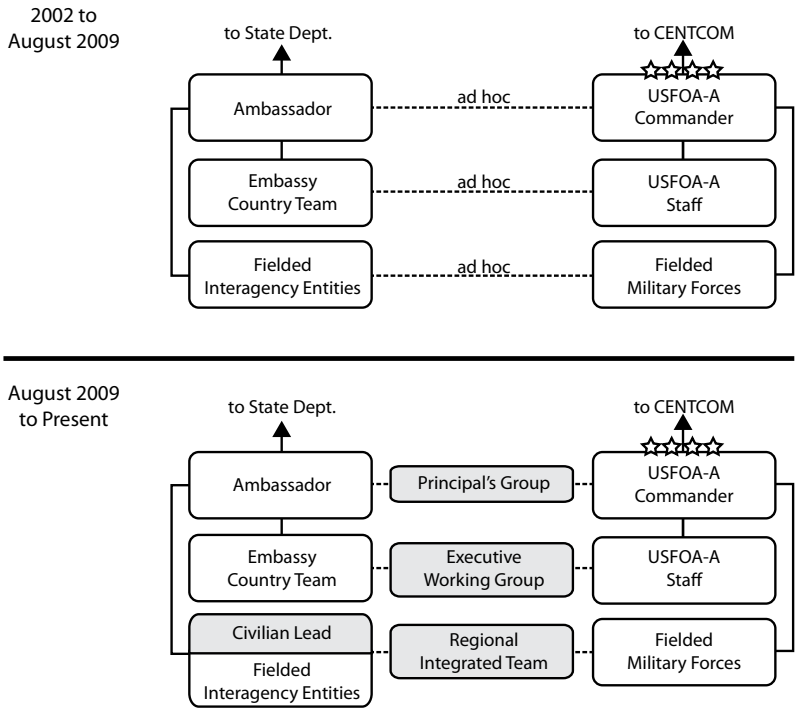

Figure 4. Past and current US organizational structures in Afghanistan

structure employed in Vietnam. Dr. Christopher Lamb, acting director of the National Defense University's Institute for National Strategic Studies, and Dr. Martin Cinnamond, who worked in a number of UN positions in Afghanistan in 2007 and 2008, called the new coordination structure insufficient, saying: "It calls for parallel chains of command with coordination at every level. Historically, however, the way to ensure civil-military cooperation is to formally integrate the military and civilian chains of command."[56]

As the previous cases demonstrate, the United States has applied a range of organizational structures to interagency operations abroad. While it can claim some success in interagency foreign endeavors, these successes are often costly in resources, time, and foreign goodwill, as the various elements of the interagency fail to work together in a synchronized manner. The next section describes four potential ways to reorganize the interagency system at the crisis task force level to produce better unity of effort.

Proposed Organizational Reforms

Since the passage of the Goldwater-Nichols DoD Reorganization Act of 1986, which unified the military services into a joint operational team,

there have been numerous studies, books, articles, and papers suggesting ways to improve interagency unity of effort.[57] After the 11 September 2001 terrorist attacks, most authors focused on problems and solutions particular to the counterterrorism mission. Following the 2003 invasion of Iraq, many changed focus to stabilization and reconstruction operations and counterinsurgency warfare. However, relatively few studies have looked at whole-of-government unity of effort across the range of COIN, counternarcotics, CT, development assistance, reconstruction and stabilization, and natural disaster response missions.

For these operational-level deliberative, or crisis-action missions, the organizational reforms proposed over the last two decades generally divide into four categories: an interagency organization, a State Department–led organization, a military-led organization, or a parallel structure. As currently practiced, the closest structures the USG has to operational-level interagency organizations are the JIATFs at SOUTHCOM and PACOM, which combine military, law enforcement, and intelligence-community personnel in a unified structure. There are no current or recent examples of State Department–led subregional interagency organizations for contingency operations, though of course the country team led by the ambassador at every US embassy provides a steady-state example of a DoS–led interagency organization. On the other hand, there are a few examples of military-led interagency organizations, including the MACV–CORDS structure in Vietnam. A parallel structure exists today in Afghanistan, with the embassy and the military joint task force (JTF) coordinating with each other but with neither formally subordinate to the other. There have also been parallel structures during humanitarian response operations, such as the response to the 2004 Asian tsunami, with the military and other agencies coordinating but with neither subordinate to the other. The following sections describe four proposed organizational reform models.

An Interagency Structure

The first operational-level reform model envisions creating an integrated interagency task force for crisis operations, unifying interagency civilian and military efforts and command structures. This structure is similar to the current JIATFs at PACOM and SOUTHCOM, though with increased command authority. The most prominent proponents of this reform model include the Defense Science Board's (DSB) 2004 summer study and the 2008 *Forging a*

New Shield and 2009 *Turning Ideas into Action* reports from the Project on National Security Reform (PNSR).

The 2004 DSB study recommended establishing joint interagency task forces composed of the leaders operating in the area of interest, including the ambassador, the USAID country director, the CIA chief of station, and other senior agency representatives. These would be augmented with DoD personnel as needed to integrate planning with higher organizational levels and ensure coordinated action by all US players.[58]

In their 2008 and 2009 reports, the PNSR team recommended creating integrated interagency crisis task forces (CTF) to conduct crisis operations. The CTFs would have an integrated civil-military chain of command, as shown in figure 5.[59] A CTF would have a single director, a clear mission, resources, and authority commensurate with assigned responsibilities. The CTF director could be either military or civilian, depending on the security situation, and would be supported by an interagency staff.[60] The CTF director would report directly to the president through the national security advisor for "large and important"[61] crises and to the director's respective department (i.e., a lead agency) for less-prominent crises. Once again, this reporting structure appears to have the potential to overload the president and National Security Council (NSC) staff. To ensure the CTF director has the necessary level of authority, the PNSR study team says CTFs should be authorized by Congress and chartered by the president.[62]

More recently, Jeffrey Buchanan et al., in a 2009 *Joint Force Quarterly* article, recommended establishing joint interagency task forces to make operational-level crisis operations both joint and interagency and provide command authority over all assigned interagency forces from the tactical level, through the JIATF commander, to a proposed regional interagency commander, to the president through the NSC.[63]

Some have recommended establishing joint government task forces (JGTF) for interagency contingency operations, led by either the military or a civilian agency, based on which organization's core competency most closely aligned with the primary mission of the task force. This means a civilian could have command of assigned military forces. The proposed JGTFs would have stronger command arrangements than the current counternarcotics JIATFs at SOUTHCOM and PACOM. In JIATF-S and JIATF-W, the task force commander has only tactical control of the participating units, while operational control remains with the parent agencies. The study recommends delegating

operational control to JGTF commanders, similar to a military-only JTF. It would also align the two current and any future standing JIATFs under the stronger JGTF model.[64] Still others recommend creating and deploying ad hoc IATFs for crisis operations. These interagency task forces would be task-organized to accomplish specific missions using the combined capabilities of the interagency and would have operational control and command authority over all forces assigned for planning, exercises, and mission execution.[65]

A 2005 article in *Policy Review* recommended developing IATFs as needed for specific missions. These integrated task forces would be led by

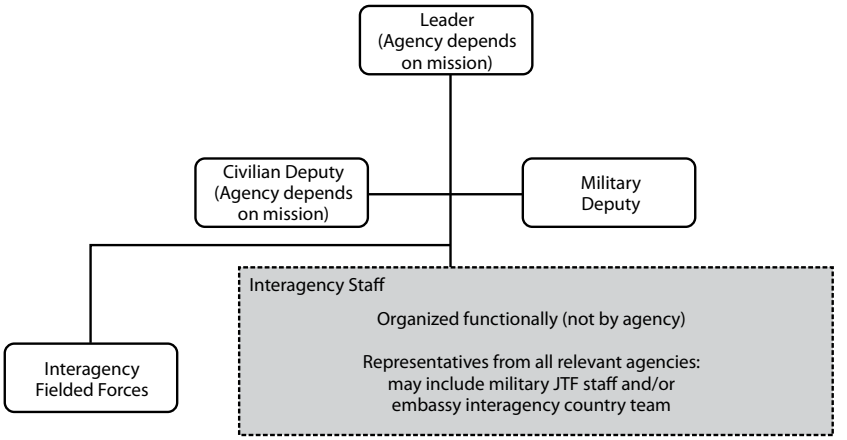

Figure 5. Interagency task force model

a presidential special representative who would report directly to the president and would have an integrated headquarters staff of representatives from all relevant agencies. The article does not specifically address how the civilian and military components would relate, but presumably they would all fall under this integrated task force. The major concern with this model is the proposal to have the task force leader report directly to the president; a handful of integrated task forces responding to crises around the globe could quickly overload the president and the NSC staff.[66]

State Department Leads

The second operational-level reform model for crisis operations would put the DoS in charge of an interagency task force. Interestingly, in two decades of reform literature there is no incidence of this model. However, the interagency country team led by the ambassador is standard for steady-state operations at all US embassies, so the model is worth considering for contingencies as well.

In a State Department lead-agency model, the USG would create an IATF similar to those described in the previous section, but the leader of the IATF would always be from the DoS. In countries with a functioning US embassy, the ambassador would be the logical choice to lead the IATF, since that position already has the responsibility to lead all US interagency activities in the country other than military forces involved in major combat operations. Where there is no functioning embassy or where the United States does not have diplomatic relations, the president could designate a special representative who would then report through DoS channels rather than directly to the president or national security advisor. This model is shown in figure 6.

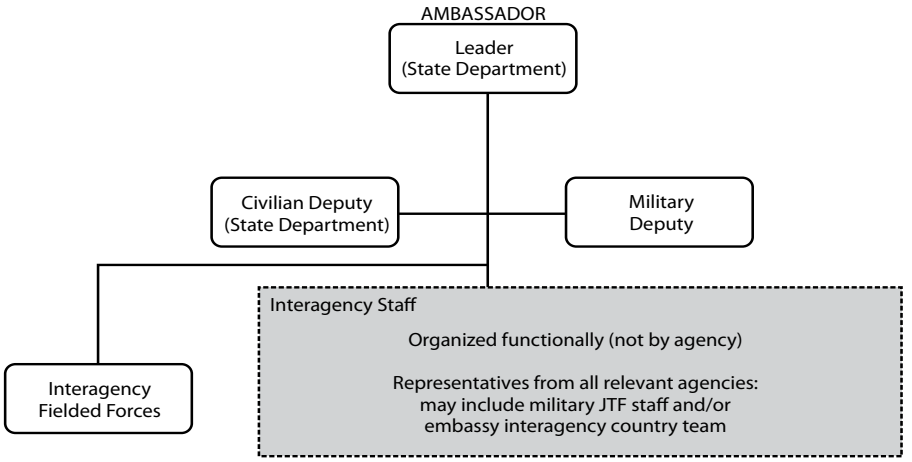

Figure 6. State Department–led interagency task force model

Under this model, the MACV–CORDS structure would have been reversed, with the civilian CORDS director in charge of the overall US effort in Vietnam and the MACV commander subordinate and providing military support to the overall effort. Similarly, in the first year after the 2003 invasion of Iraq, Coalition Provisional Authority (CPA) administrator and presidential special representative (and ambassador) L. Paul Bremer would have been in charge of the overall US effort in Iraq with the military JTF in support, rather than the uncoordinated parallel structure that existed. The rationale for this proposal is that in complex operations, such as counterinsurgencies or postconflict stabilization and reconstruction, the desired end state is political, not military. While security is a necessary part of the overall effort, the years of frustration during America's efforts in Vietnam, Iraq, and Afghanistan demonstrate that great military effort is often expended to achieve little in the way of strategic goals if it is not firmly di-

rected toward the overall political objectives. This model would attempt to put the right senior civilian with the right understanding of broad US goals in charge of the response.

Military Leads

The third reform model for crisis operations would put the military in charge of an interagency task force, as the United States did with the MACV–CORDS structure in Vietnam. Again, it is interesting to note that there has been very little discussion in the literature about this model, despite the fact that many historians and military analysts have praised the CORDS structure in Vietnam.

The only proposal of this type identified in the literature comes from a 2006 paper advocating a CORDS–like construct. The State Department's S/CRS would create a civilian interagency organization that would be a subordinate part of a military JTF, as was done by MACV–CORDS in Vietnam (The military-led structure is shown in fig. 7). This study contends this would be better than the current JIACG and JIATF models, which try to achieve unity of effort without unity of command, and would also be better than the parallel structure frequently used today. The parallel structure mirrors the unsuccessful arrangement the US used in Vietnam prior to the establishment of the CORDS.[67]

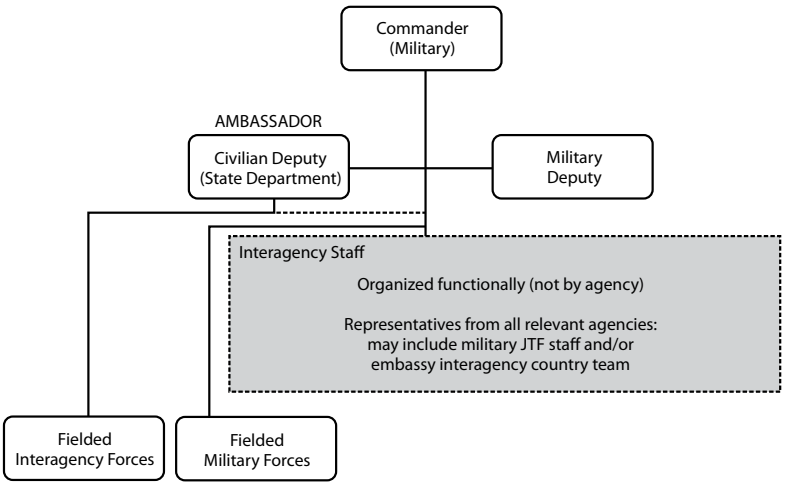

Figure 7. Military-led IATF model

A Parallel Structure

Finally, the fourth model would use a parallel civil-military structure with neither in charge of the overall effort. The most significant proponent of this structure is the Center for Strategic and International Studies (CSIS); few others have proposed this model. The PNSR study team contends that "dual civilian and military chains of command in the field complicate unity of purpose and effort."[68]

Lt Col Harold Van Opdorp, USMC, in a July 2005 *Small Wars Journal* article, proposed a classic parallel structure, creating a "deployable JIACG" that would unify the civilian interagency presence in a country under a single organization that would operate in parallel with the military's JTF.[69] Depending on the situation, either the deployable JIACG or the JTF would be the supported command with the other acting in support. During major combat operations, the JTF would be the supported command, while in a humanitarian response operation, the deployable JIACG would most likely be the supported command. Van Opdorp notes that many operational plans incorporate phases, and the supported/supporting relationship between the deployable JIACG and the JTF could change as the campaign phases change; for instance, the JTF passes the leading role to the deployable JIACG during the transition to postconflict stabilization and reconstruction operations.[70]

The CSIS study team proposed a much more integrated task force structure but one which still has two leaders reporting in two separate chains of command to Washington, albeit with an integrated staff and a great deal of coordination. The CSIS team recommended establishing an IATF to integrate the day-to-day efforts of all US agencies participating in a crisis operation. The IATF would deploy to the field and would be jointly led by a military JTF commander and a civilian special representative appointed by the president.

The president's special representative, who could be the US ambassador or another senior civilian of comparable stature, would be responsible for achieving the overall US objectives and would have directive authority over all US government civilians deployed to the field for the operation. The special representative would report to the president through the secretary of state. The JTF commander, a senior military officer, would be responsible for military operations, would have operational control over all US military forces deployed to the field for the operation, and would report to the geographic combatant commander, leaving the traditional military chain of command unbroken. While the special representative

would have no direct authority over the JTF commander, he or she would be able to raise disagreements to the NSC or the president for resolution.

Both the special representative and the JTF commander would be supported by a single, integrated interagency staff, composed largely of military personnel under the command of the JTF commander plus civilian personnel detailed from various agencies to work for the special representative. Where a functioning US embassy exists, the integrated staff would augment the existing country team, which would then become the support staff for the operation.[71] The parallel structure proposed by the CSIS team is shown in figure 8.

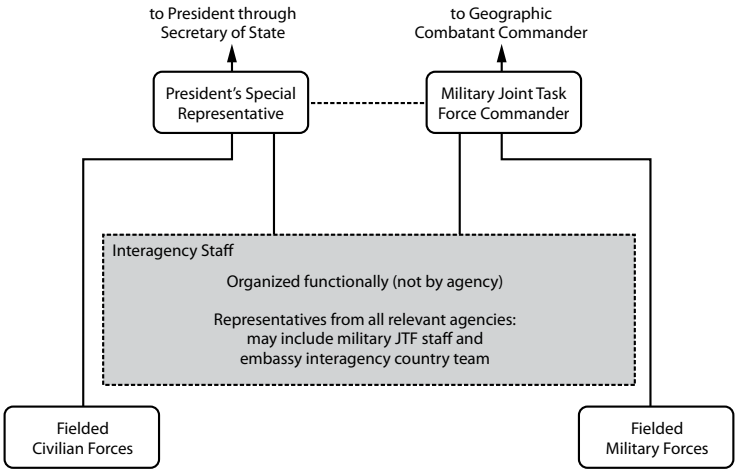

Figure 8. Parallel-structure interagency task force model

Analysis and Recommendation

Past and current examples of organizational structures used by the United States across the range of counterinsurgency, counternarcotics, counterterrorism, development assistance, reconstruction and stabilization, and natural disaster response missions are instructive. Examining the four proposed organizational reform models leads to the question of what criteria should drive the change of interagency operations.

Criteria for Change

From the many criticisms brought against the current interagency structure and the identified problems in both recent and ongoing operations, this article now proposes criteria by which to evaluate interagency reforms. Ideally, a better interagency structure would accomplish 13 things.

First, many observers argue that the military's role in foreign policy is too large, so a reform must be found that increases the ability of the DoS to lead US foreign policy across the interagency while lowering the military's profile. Assistant Secretary of State for Political-Military Affairs John Hillen stated in 2005, "If we subvert, however unintentionally, our ability for the lead foreign policy agency of the US government [i.e., the DoS] to deliver credible and consistent messages . . . to those actors whose behavior we are trying to shape and change, we will lose influence and legitimacy."[72] Also, a 2006 Senate Foreign Relations Committee investigation concluded, "There is evidence that some host countries are questioning the increasingly military component of America's profile overseas."[73] Similarly, in June 2008, Secretary Gates warned against the "creeping militarization" of foreign policy and advocated for a larger role for the State Department.[74] More recently, chairman of the Joint Chiefs of Staff (CJCS) ADM Michael Mullen stated, "US foreign policy is still too dominated by the military."[75]

Second, the reform must produce better-coordinated planning at the operational level than is now achieved. There are numerous examples, such as the 1989–90 intervention in Panama and the 2003 invasion of Iraq, in which lack of coordination between agencies during the planning phase led to significant problems during execution, particularly when the military perceived it was time to transfer responsibility for the operation to another agency. In Operations Just Cause and Promote Liberty in Panama, the military began contingency planning for regime change and postconflict operations in 1987, but for reasons of operational security did not discuss the plans with other agencies it assumed would play key roles until days before the December 1989 invasion.[76] In Operation Iraqi Freedom, planners from the military, the DoS, and the USAID developed separate postconflict plans. Ultimately, the plan the United States intended to follow for postconflict operations in Iraq was developed by the DoD, beginning in January 2003, without coordination with previous State Department or USAID efforts.[77] This lack of coordinated planning contributed to a slow start to US postconflict operations in Iraq, opening the way for the insurgency that developed.

Third, the reform also must produce interagency unity of effort during execution. Uncoordinated actions are wasteful of time and resources and can make it more difficult to accomplish US goals. For example, if the Army Corps of Engineers builds a school but the USAID does not assist

with funding for teacher training, the effort was wasted and may even be counterproductive if it leads the local population to doubt US abilities or commitment. A lack of unity of effort characterizes much of the US experience in Iraq. A 2009 GAO study stated, "Since 2005, multiple US agencies—including the State Department, USAID, and DoD—led separate efforts to improve the capacity of Iraq's ministries to govern, without overarching direction from a lead entity to integrate their efforts."[78]

Fourth, any move to reorganize interagency structures and processes must lead to a system which is more effective—and perhaps more efficient—than the various agencies working alone, without the extra bureaucratic and resource overhead associated with interagency coordination.[79] Increased effectiveness is absolutely required, or the reform is counterproductive. Improved efficiency, while not required, is desirable. The PNSR study team notes that the current system "militate[s] against efficiency and effectiveness by undermining cooperation and collaboration . . . [in which competition] and information hoarding between agencies and their personnel is often standard behavior."[80]

Fifth, the reform should task leaders with clear responsibilities and give them the necessary authority to carry out those responsibilities. Prominent management theorist Lyndall Urwick coined two applicable concepts: the principle of authority, which says there should be a clear line of authority from the top of a management structure to every individual, and the principle of correspondence, which says a leader must be given authority commensurate with assigned responsibility. He argued that, no matter how complex the organization, these principles should be observed.[81] Too often, today's system of interagency coordination assigns responsibility but does not clearly define a chain of command or provide a leader with the needed level of authority over personnel, resources, or processes of other agencies.

Sixth, the decisions made by the leader or leaders must be perceived as legitimate and authoritative by participants outside the leader's home agency. Organizational reform expert and current Air Force secretary Michael Donley[82] notes, "Lack of complete authority and murky, unclear divisions of responsibility mean that legitimacy in decision making will be challenged."[83] This is often the case in today's system, where decisions by a leader from one agency are not perceived as binding by another executive branch agency.

Seventh, the leaders of the interagency process must have access to the necessary financial, personnel, and material resources from other agencies

to be successful in their assigned mission. For example, the DoS or the USAID is often tasked to accomplish a diplomatic or developmental mission, which it cannot achieve without the logistical or security resources provided by the military. In some cases, this issue will require congressional changes, as budgets are provided by Congress to individual agencies, and the executive branch has limited authority to realign resources among agencies.

Eighth, the leader and organization must have a clear chain of command to the president, who is the ultimate decision maker on foreign policy and national security issues. This is again Urwick's principle of authority, which requires a clear line of authority from top management to every individual. Structures which report generically to "the NSC" or in which multiple leaders in the field report to different leaders in Washington contribute to either undefined or multiple competing chains of authority to the president, violating this principle.

Ninth, the structure must not overburden the president and the national security advisory team, who need to be focused on strategic goals and policies rather than crisis decision making. The PNSR study team notes, "White House centralization of interagency missions . . . risks creating an untenable span of control over policy implementation . . . [This] tends to burn out National Security Council staff, which impedes timely, disciplined, and integrated decision formulation and option assessment . . . [and] almost guarantees an inability to do deliberate, careful strategy formulation." Any reform of the interagency system "must free the president and his advisors for strategic direction by providing effective mechanisms for decentralizing national security issue management."[84]

Tenth, the reform should fix the imbalance of bureaucratic power and prestige between the Departments of State and Defense. The State Department is much smaller in terms of both budget and personnel than the Defense Department. The DoD has an annual budget of about $660 billion and a workforce of approximately three million, while the DoS has an annual budget of about $50 billion and a workforce of fewer than 60,000 people, of whom only 6,400 are FSOs.[85] The additional power is required to ensure the State Department's voice is heard during interagency deliberations, and additional prestige is required for the DoS to be able to obtain increased funding and personnel from Congress. Even Secretary Gates has argued that the DoS needs additional resources and capacity to participate in the interagency process, saying whole-of-government

approaches "can only be done if the State Department is given resources befitting the scope of its mission."[86]

Eleventh, for the coordinated interagency system to improve its capabilities over time, personnel from across the participating agencies need both training and experience working with other agencies. Reform options that routinely place working-level personnel from different agencies in contact with each other are more likely to produce this than stove-piped agencies working in parallel or achieving coordination only through small interagency cells.

Twelfth, any changes to the interagency system should minimize the financial, personnel, and materiel costs required to establish the new system. With a constrained federal budget, advocating any reforms to Congress and the various interests in Washington will be difficult if costs increase.

Finally, changes to the interagency system should attempt to minimize culture shocks in the participating agencies. Much has been written about the different cultures in the various organizations, particularly between the military and the DoS.[87] Reforms will be easier to advocate and implement if working-level personnel in the participating agencies do not perceive the new procedures as threats to their careers or their sense of self. Cultures can be transformed, but it takes a great deal of time and effort.

Evaluation and Recommendation

The most robust version of each of the four proposed structures was considered during the evaluation and assessed against the 13 criteria for change. Despite the derivation of a numeric score for each alternative, the evaluation scheme is qualitative and subjective. Though this model weights all criteria equally, it could be argued that some factors are more important than others. This analysis deliberately avoided that complication. The ratings for each of the four models are summarized in table 1.

The analysis reveals that an integrated interagency task force with a leader from the agency most appropriate to the mission is the best choice. The parallel structure used most often today is the worst of the four models, while the two lead-agency models fall somewhere in between.

The United States should establish integrated IATFs for crisis operations and enduring regional interagency missions such as counternarcotics. Each IATF would have a single director, a clear mission, resources, and authority commensurate with assigned responsibilities. The IATF director could be either military or civilian, depending on the security situation and which agency's core competency most closely aligned with the primary mission

Table 1. Analysis of operational-level interagency models

Evaluation Criteria	*Interagency Organization*	*DoS Leads*	*Military Leads*	*Parallel Structure*
Nonmilitary voice and face for US foreign policy	0	+	–	0
Fully-coordinated planning	+	+	+	0
Unity of effort during execution	+	+	+	0
More efficient and effective than agencies working alone	+	+	+	0
Leader's authority commensurate with responsibility	+	0	0	–
Legitimacy of leader's decision making	+	0	0	+
Leader can access necessary resources	+	0	0	0
Clear chain of command to the president	+	+	+	–
Does not overburden the president	+	0	0	–
Balance of power and prestige between DoD and DoS	0	+	–	–
Develops interagency expertise	+	+	+	0
Reform minimizes cost in money, personnel, and materiel	0	0	0	+
Reform minimizes agency culture shocks	0	–	0	+
TOTALS	+9	+6	+3	–1

of the task force, and could be designated as a presidential special representative if necessary to provide the leader more rank and authority, both internationally and domestically within the interagency. The IATF director would be supported by an interagency staff using an integrated civil-military chain of command. The IATF would be provided with the necessary personnel and resources from across the interagency, including the military, and the director would have operational control over all assigned forces.

Implementation Considerations

The IATF model would have worked in each of the aforementioned scenarios, but is especially applicable for current operations in Afghanistan. It likely would have avoided many of the problems the United States has faced through years of uncoordinated operations. Once the US Embassy was reopened in Kabul, civilian and military elements in Afghanistan

could have functioned as an IATF under overall supervision of the ambassador, with the commander of US military forces in Afghanistan as the ambassador's military deputy, producing unity of effort through unity of command rather than the personality-driven parallel structures, which have existed through most of the US involvement there. Alternatively, the IATF might include a larger operating area comprising both Afghanistan and Pakistan. In this case, the IATF director could be the president's special representative for Afghanistan and Pakistan, and the IATF would include the US embassies in both countries, as well as conventional military forces, special operations forces, and CIA covert action elements in both countries.

However, one must consider the requirements necessary to implement the new IATF model. These include overcoming bureaucratic resistance, obtaining diplomatic acceptance for this new construct from the rest of the world, minimizing the cost of the reform and finding a way to pay for it, addressing issues of agency culture and training interagency personnel, and obtaining congressional support and action.

Bureaucratic Resistance

One issue to address when implementing any reforms in USG executive agencies is the entrenched power of bureaucracies and their desire to preserve the status quo. While many military authors have proposed interagency reforms, relatively few proposals come from the State Department. This may be an indicator that those who hold bureaucratic power at the DoS are not in favor of reform along the lines advocated in this article. For example, the CORDS interagency construct used during the Vietnam War was largely supported by the DoD but opposed by non-DoD agencies, which continually tried to reduce the funding, personnel, and mission assigned to the CORDS.[88] Similarly, today there are those in the State Department—particularly in the Bureau of African Affairs and at US embassies across Africa—who do not support the establishment of the military's new US Africa Command.[89]

DoS leaders may be concerned that the new IATF construct will require too many scarce DoS personnel and resources, making it impossible to properly staff and resource existing missions. This concern would best be addressed by increasing the State Department's budget and number of personnel, as Secretary Gates, CJCS Mullen, and many others have advocated for years.

Another group which may resist this reform is the American Foreign Service Association—the bargaining organization which protects the interests of US Foreign Service officers. FSOs may be concerned about the effects of these reforms on their career paths, such as whether interagency service will derail their careers or whether it will be required to advance to senior ranks in the Foreign Service. These concerns could be addressed by clearly describing the new career tracks for FSOs and offering suitable promotion, monetary, or other incentives for accepting these career paths.

Leaders in other agencies may also resist the new interagency construct because their personnel would report to leaders from another agency when serving at the IATFs, which would be perceived as a diminution of their power. As with the State Department, addressing the concerns of these leaders could include providing additional personnel and funding, clarifying and codifying their roles and authorities, and clearly delineating career paths in these agencies which lead to senior levels of leadership.

Diplomatic Acceptance

Achieving diplomatic acceptance from the rest of the world for this new construct is important but should not be a major challenge. When the United States conducts noncombat actions such as disaster relief, many host nations would prefer to work with an IATF headed by a USAID OFDA representative, for example, than one headed by a military officer. Similarly, in complex reconstruction and stabilization operations, host nations would probably perceive an IATF headed by a senior diplomat or development specialist, rather than a military officer, as more of an offer of assistance and less of a threat to their sovereignty. In those (hopefully few) cases of US military action in a nonpermissive environment, the IATF would likely be led by a military officer—at least initially—which would be welcomed by threatened governments in the region, while the perceptions of the target nation would be largely irrelevant.

Cost

Any reform of the interagency system becomes more difficult, or even impossible, as the projected cost increases. While it is beyond the scope of this article to conduct a detailed cost assessment of this reform, some ballpark estimates can be offered. Implementing the model should cost relatively little, since the envisioned IATFs would frequently be military-heavy organizations like today's JTFs and JIATFs, with the addition of interagency

personnel from embassy country teams, which currently often operate in parallel with the military structure. Thus, the IATF largely would use the same personnel and resources as in past and current operations but in a more integrated structure. A modest number of additional personnel from other agencies would be required; as few as 10 or 20 for a small operation to as many as a few hundred for a large, complex operation like the CPA's administration of Iraq prior to returning sovereignty to the Iraqi government. At any given time, from two to 10 IATFs would most likely be active around the world, leading to a surge requirement of perhaps 100–1,000 non-DoD personnel across the interagency, which would cost in the neighborhood of $10–100 million in annual salaries, plus training, pensions, and other expenses.[90] However, if legislation were to shift this number of personnel billets from the DoD to the other agencies, this could be cost neutral, except for the additional training required. Shifting the billets makes sense, since the increased presence of the interagency in these operations would be expected to reduce the military workload, and the 1,000 DoD billets is less than one-tenth of one percent of its three million personnel.

Personnel and Culture

While funding the new model may not be difficult, recruiting and training the necessary new personnel for the non-DoD agencies could be much more challenging, since the skill sets in these agencies tend to require higher initial education than the average entry-level military position. It might take several years to recruit the necessary personnel and train them at the Foreign Service Institute, National Defense University, or other interagency schools.

Of perhaps greater importance is developing a true interagency career path. The 2006 *Quadrennial Defense Review* (*QDR*) concurred, saying that "interagency operations would be strengthened by establishing a national security officer career path."[91] The 2010 *QDR* also addressed this issue, recommending that Congress "allocate additional resources across the government and fully implement the National Security Professional (NSP) program to improve cross-agency training, education, and professional experience opportunities."[92]

The Goldwater-Nichols Act created the joint military team, in part by requiring that all flag-rank military personnel have experience in a qualifying joint position. The combatant commands, the Joint Staff, and the many joint task forces also provide numerous opportunities for military

officers to gain experience working in the joint military environment at various points in their careers. While mandated interagency experience may or may not be required to qualify for senior leadership positions, the new IATF model would have to offer opportunities at several points in an individual's career to gain interagency experience at the working level, line supervisory level, and senior level if the United States hopes to create a cadre of experienced interagency professionals. Such a cadre would also benefit from opportunities to attend professional interagency education, analogous to professional military education, at one or more points in an interagency civilian's career. This would incur costs both for a school and instructors and for enough surplus personnel in comparatively small agencies to allow personnel to attend school while all critical billets remain filled.

It is also necessary to make interagency service an acceptable and even valued part of each participating agency's culture. Today, many professionals in the non-DoD agencies are strongly partial to their agency's culture and prefer to work only within that agency. Over time, this cultural isolation would need to change. A defined interagency career path and opportunities to attend school with personnel from other agencies would help, but most of all, this change would simply take time to evolve.

Congressional Support and Legislation

Large changes to the national security system above the single agency or department level would most certainly require action by the president and Congress. Some have argued that a presidential executive order would be sufficient to enact the proposed reforms.[93] While an executive order might change the interagency system during the current administration, history indicates it would be unlikely to remain under the next president.[94] For example, President Clinton's new process for interagency reconstruction and stabilization operations, described in Presidential Decision Directive-56 (PDD-56), did not outlast his presidency, nor was it generally followed while he was in office.[95] Nor does an executive order presuppose any support from Congress, which funds the executive branch agencies. Because political power in Congress is often strongly tied to the large sums of money associated with the defense budget, Congress will certainly want to be involved in any reforms that change the national security structure. The CSIS "Beyond Goldwater-Nichols" study team noted: "The role of Congress in the process is the most crucial determinant of the prospects for a reform effort. The recommendations that flow from congressionally

mandated groups, commissions, or blue ribbon panels are more likely to lead to lasting changes than efforts launched exclusively at the executive branch level."[96]

Enduring change comes from legislation. Examples include the 1947 National Security Act which created, among other things, the National Security Council and the Department of Defense; the 1986 Goldwater-Nichols Act which created the joint military team; the 2002 act which created the Department of Homeland Security; and the 2004 act which created the office of the Director of National Intelligence.

Proper resourcing also comes from legislation. Michael Donley argues that if a new interagency structure is established in statute, "Congress has a more visible obligation to provide supporting institutional resources."[97] The CSIS study team states that "Legislation could also provide the basis for realigning agency authorities and resources to ensure that each agency has the capabilities it needs to execute its assigned tasks."[98] Because many of the complex operations which would benefit from execution by an IATF are unpredictable crises, budgeting for these IATFs would require some guesswork and flexibility by both Congress and executive branch agencies. The DoS and USAID budgets could include contingency funds in anticipation of a certain number of IATF operations each year, or funds could be provided to participating agencies through supplemental appropriations for particular crisis operations, as Congress has done for US operations in Iraq and Afghanistan. To facilitate unity of effort, the legislation authorizing these funds should include language which enables the transfer of funds between agencies and provides the IATF leader with some ability to prioritize interagency efforts and direct funding transfers when necessary within specified limits. To ensure oversight of these transfers, the legislation could require congressional notification of any transfers over a specified amount. While the capability for the IATF leader to direct transfer of funds would be new, the process of interagency funding transfer itself is not without precedent. For example, Section 1207 of the FY-06 National Defense Authorization Act permitted the DoD to transfer to the DoS "up to $100 million in defense articles, services, training or other support for reconstruction, stabilization, and security activities in foreign countries," and the Pakistan Counterinsurgency Capability Fund, established by the FY-09 Supplemental Appropriations Act, permits the DoS to transfer all monies appropriated for this fund to the DoD or other federal agencies

so they can conduct operations to build and maintain the capability of Pakistani counterinsurgency forces.[99]

Finally, legislation would be needed to place new interagency civilian leaders, such as a USAID OFDA expert leading a disaster-response IATF, in command of participating military forces and personnel from other US agencies. The United States already practices civilian control of the military, with the president and secretary of defense in charge of the military during both peace and war and the civilian secretaries of the Air Force, Army, and Navy in charge of each service's organize, train, and equip (i.e., peacetime) missions. Additionally, US ambassadors direct interagency country teams, which generally include some military personnel at their respective embassies. So, the concept of placing civilians in charge of military personnel or personnel from one agency in charge of personnel from another is not without precedent. As with interagency funding issues, Congress could specify authorities and limitations in authorizing the IATF and could provide oversight through the congressional hearings process. Participating executive branch agencies could also elevate concerns and disputes to the National Security Staff and National Security Council process for resolution, when necessary, though it is hoped these disputes would decrease both in intensity and frequency as participating agencies become more comfortable with IATFs.

Obtaining congressional approval for the new reforms would not be easy. Previous reforms occurred largely in response to lessons learned from World War II, the failed hostage rescue mission in Iran, and the 9/11 attacks. Significant lessons from more than two decades since Goldwater-Nichols could motivate the necessary reforms, but these have not yet been enough to influence the president or Congress to devote political capital to a reform effort. Attempting changes across multiple agencies is particularly difficult in Congress because authority over the various agencies is distributed across multiple committees in the House and Senate. This not only requires the action of many different committees but also the understanding that power in the committees may shift based on the reform. For example, the proposed reforms would likely strengthen the House and Senate Foreign Relations Committees significantly, while diminishing the power of the Armed Services Committees.[100]

There is at least some interest in Congress in assessing and addressing the lack of interagency unity of effort. On 30 April 2009, Rep. Randy Forbes (R-VA) sponsored the Interagency Cooperation Commission Act,

which would "establish a commission to examine the long-term global challenges facing the United States and develop legislative and administrative proposals to improve interagency cooperation."[101] However, the bill has no cosponsors and has been stalled in the House Oversight and Government Reform Committee, Subcommittee on Government Management, Organization, and Procurement, since 26 June 2009, with no plans for further action on the bill. Given the many other significant issues facing Congress at the time of this writing, coupled with the US drawdown in Iraq in 2011 and the anticipated drawdown in Afghanistan by 2014, there may simply not be enough congressional attention or interest to tackle a reform of this magnitude in the near future.

Conclusion

The US government conducts a range of deliberate and crisis-action operations abroad, including counterinsurgency, counternarcotics, counterterrorism, development assistance, reconstruction and stabilization, and natural disaster response. Expertise for these missions is spread across executive branch agencies, and generally, no single agency can accomplish these complex missions alone. In complex operations with participants from more than one US agency, coordinated planning and execution at the operational level is often lacking, leading to redundancies, gaps, friction, and frustration.

Organizational reforms proposed over the last two decades for these operational-level deliberate or crisis-action missions divide into four categories: an interagency organization, a State Department–led organization, a military-led organization, or a parallel structure. A comparative analysis of these four models, using 13 evaluation criteria, indicates an integrated interagency task force is the best organizational model for these operations. It also indicates that the parallel structure used most often today is the worst of the four models, while the two lead-agency models fall somewhere in between.

The United States should establish integrated IATFs for crisis operations and enduring regional interagency missions. Each IATF would have a single director, a clear mission, and resources and authority commensurate with assigned responsibilities. The IATF director could be either military or civilian, depending on the security situation and which agency's core competency most closely aligns with the primary mission of the task force, and

could be designated as a presidential special representative to give the leader greater rank and authority, both internationally and domestically within the interagency. The IATF director would be supported by an interagency staff using an integrated civil-military chain of command. The IATF would be provided with the necessary personnel and resources from across the interagency, including the military, and the IATF director would have operational control over all assigned forces.

There are challenges to implementing this reform—including overcoming bureaucratic resistance, obtaining the diplomatic acceptance from the rest of the world for this new construct, minimizing the cost of the reform and finding a way to pay for it, addressing issues of agency culture and training interagency personnel, and obtaining congressional support—but none which cannot be surmounted. The new IATF construct would be substantially more effective in achieving US foreign policy and national security goals. It makes sense to expend the necessary effort. SSQ

Notes

1. US Agency for International Development, "USAID Afghanistan: US Government Agencies," http://afghanistan.usaid.gov/en/Page.USG.aspx.
2. Richard W. Stewart, "Winning Hearts and Minds: The Vietnam Experience," in *Mismanaging Mayhem: How Washington Responds to Crisis*, eds. James Jay Carafano and Richard Weitz (Westport, CT: Praeger Security International, 2008), 90.
3. Ibid.; and Maj Ross M. Coffey, USA, *Improving Interagency Integration at the Operational Level: CORDS—A Model for the Advanced Civilian Team* (Fort Leavenworth, KS: School of Advanced Military Studies, 25 May 2006), 24.
4. Maj Gen George S. Eckhardt, *Vietnam Studies: Command and Control, 1950–1969* (Washington: Department of the Army, 1991), 27, 29, 48, 69.
5. Coffey, *Improving Interagency Integration at the Operational Level*, 19, 24.
6. Ibid., 24, 26; and Stewart, "Winning Hearts and Minds," 90–91.
7. Stewart, "Winning Hearts and Minds," 94.
8. Coffey, *Improving Interagency Integration at the Operational Level*, 28–29.
9. Stewart, "Winning Hearts and Minds," 105–6.
10. Ibid., 106.
11. Coffey, *Improving Interagency Integration at the Operational Level*, 3–4. See also John T. Fishel, "The Interagency Arena at the Operational Level: The Cases Now Known as Stability Operations," in *Affairs of State: The Interagency and National Security*, ed. Gabriel Marcella (Carlisle, PA: Strategic Studies Institute, December 2008), 420–21.
12. US Joint Forces Command (JFCOM), "Provincial Reconstruction Teams," Joint Warfighting Center predoctrinal research white paper no. 07-01, 21 November 2007, 14.
13. Ibid.
14. Joint Publication (JP) 3-07.4, *Joint Counterdrug Operations*, 13 June 2007; JP 3-05.1, *Joint Special Operations Task Force Operations*, 26 April 2007; and JP 3-40, *Combating Weapons of Mass*

Destruction, 10 June 2009. JP 3-07.4 briefly describes JIAFT-S and JIATF-W but gives no broader doctrinal applications of JIATFs. JP 3-05.1 describes the JTF as the operational focal point for interagency coordination and mentions that the JTF may be assigned a subordinate JIATF to assist with interagency coordination. JP 3-40 provides the brief statement above but then notes "JIATFs currently do not have authority to conduct WMD interdiction."

15. JFCOM, "Provincial Reconstruction Teams," 14.

16. Ibid.

17. JFCOM, "Insights & Best Practices: Interagency, Intergovernmental, and Nongovernmental Coordination (A Joint Force Operational Perspective)," Joint Warfighting Center focus paper no. 3, July 2007, 14–15.

18. Ibid.

19. Recently, the North Atlantic Treaty Organization's International Security Assistance Force (NATO ISAF) and US Forces Afghanistan (USFOR-A) established three combined joint interagency task forces (CJIATF) to focus on the complex "nexus of insurgency, narcotics, corruption, and criminality" in Afghanistan. These include CJIATF-Nexus, CJIATF-435, and CJIATF-Shafafiyat. There is little information available about these new task forces, and even some question whether all three are actually CJIATFs under a subordinate commander or if they are elements of the USFOR-A, ISAF, or embassy staff. DoS, Bureau of South and Central Asian Affairs, "US Counternarcotics Strategy for Afghanistan," 24 March 2010.

20. Fishel, "Interagency Arena at the Operational Level," 427–28.

21. US Pacific Command (PACOM), "Joint Interagency Task Force-West," http://www.pacom.mil/staff/JIATFWest/index.shtml. See also JP 3-07.4, *Joint Counterdrug Operations*, I-2; and Edward Marks, "PACOM, JIACG, and the War on Terror," Camber Corporation on contract to the Joint Interagency Coordinating Group on Counterterrorism, PACOM, 18 August 2005, 17.

22. PACOM, "Joint Interagency Task Force-West."

23. Fishel, "Interagency Arena at the Operational Level," 427–28.

24. JP 3-07.4, *Counterdrug Operations*, I-2.

25. Richard M. Yeatman, "JIATF-South: Blueprint for Success," *Joint Force Quarterly* no. 42 (3rd Qtr. 2006): 27.

26. Fishel, "Interagency Arena at the Operational Level," 427–29; and Yeatman, "JIATF-South," 26.

27. Marcy Stahl, *Joint Interagency Coordination Group (JIACG) Training and Education Survey Results* (Vienna, VA: Thought Link, Inc., 15 January 2004), 43, www.thoughtlink.com/ppt/ TLI-JIACGSurvey-FinalBrief-Revised.ppt.

28. Fishel, "Interagency Arena at the Operational Level," 429; JFCOM, "Insights & Best Practices," 15; and LCDR Tom Stuhlreyer, USCG, "The JIATF Organization Model: Bringing the Interagency to Bear in Maritime Homeland Defense and Security," *Campaigning* (Spring 2007), 42–43.

29. Fishel, "Interagency Arena at the Operational Level," 439. See also Yeatman, "JIATF-South," 26.

30. Stuhlreyer, "JIATF Organization Model," 43.

31. US Government Accountability Office (GAO), *Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing*, GAO-09-904SP (Washington: GAO, September 2009), 26.

32. Fishel, "Interagency Arena at the Operational Level," 429.

33. Stuhlreyer, "JIATF Organization Model," 42.

34. Gary W. Anderson, " 'Interagency Overseas': Responding to the 2004 Indian Ocean Tsunami," in *Mismanaging Mayhem*, 193.

35. Ibid., 194, 202.

36. Ibid., 195–96, 202.

37. Ibid., 195, 197–98, 202.

38. Ibid., 195, 204.

39. Ibid., 196, 198, 203.

40. A joint interagency coordination group (JIACG) is an element of a military combatant commander's staff composed of representatives from other USG agencies. These interagency personnel provide advice to the combatant commander and his staff, but cannot coordinate on behalf of their parent agency or commit personnel or resources from their parent agency. See JFCOM, *Commander's Handbook for the Joint Interagency Coordination Group (JIACG)* (Norfolk, VA: JFCOM Joint Warfighting Center, 1 March 2007).

41. Anderson, "Interagency Overseas," 195, 203.

42. Ibid., 194–95, 200.

43. Seth Jones, *In the Graveyard of Empires: America's War in Afghanistan* (New York: W. W. Norton & Co., 2009), 142.

44. Ibid., 139; and JFCOM, "Insights & Best Practices," 13.

45. Christopher J. Lamb and Martin Cinnamond, "Unified Effort: Key to Special Operations and Irregular Warfare in Afghanistan," *Joint Force Quarterly* no. 56 (1st Qtr. 2010): 44.

46. Jones, *In the Graveyard of Empires*, 150.

47. Lamb and Cinnamond, "Unified Effort," 43–44.

48. LT Joshua W. Welle, USN, "Civil-Military Integration in Afghanistan: Creating Unity of Command," *Joint Force Quarterly* no. 56 (1st Qtr. 2010): 56. Lieutenant Welle was a civil-military planner for ISAF Regional Command South from November 2008 to August 2009.

49. US House of Representatives, House Armed Services Committee, Subcommittee on Oversight and Investigations, "Agency Stovepipes vs. Strategic Agility: Lessons We Need to Learn from Provincial Reconstruction Teams in Iraq and Afghanistan," Committee Print 8, April 2008, 32.

50. Greg Bruno, "Afghanistan's National Security Forces," Council on Foreign Relations backgrounder, 16 April 2009.

51. Secretary of Defense Robert M. Gates at a 13 April 2009 NATO summit; quoted in Lamb and Cinnamond, "Unified Effort," 41.

52. GEN David Petraeus replaced GEN Stanley McChrystal as USFOR-A commander on 4 July 2010, though the civil-military structure established by Ambassador Eikenberry and General McChrystal remains relatively unchanged. However, the personal relationship between top civilian and military leaders and the commitment to unity of effort has improved.

53. Beth Cole and Emily Hsu, "Guiding Principles for Stability and Reconstruction: Introducing a New Roadmap for Peace," *Military Review* (January/February 2010): 15.

54. US Embassy–Kabul and USFOR-A, *United States Government Integrated Civilian-Military Campaign Plan for Support to Afghanistan* (10 August 2009), 29–30, ii.

55. Ibid., 28–30.

56. Lamb and Cinnamond, "Unified Effort," 50.

57. The most significant prior studies on improving interagency unity of effort include the 2001 Hart-Rudman Commission report by a panel of DoD–chartered outside experts, the 2004 Defense Science Board study by another panel of DoD–chartered outside experts, the 2004 9/11 Commission report by a congressionally chartered bipartisan panel, the 2005 "Beyond Goldwater-Nichols" report from the CSIS, and the 2007 "State Department in 2025" study by a panel of DoS–chartered experts. Most recently, the Project on National Security Reform produced the 2008 *Forging a New Shield* and 2009 *Turning Ideas into Action* reports in response to

a requirement of the 2008 National Defense Authorization Act, which mandated a study of the interagency national security system by an independent, bipartisan organization. The US Commission on National Security/21st Century (Hart-Rudman Commission), *Road Map for National Security: Imperative for Change, Phase III Report*, 31 January 2001; Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *Defense Science Board 2004 Summer Study on Transition to and from Hostilities* (Washington: GPO, December 2004); *The 9/11 Commission Report*, 22 July 2004, http://www.9-11commission.gov/report/911Report.pdf; Clark A. Murdock and Michèle A. Flournoy, *Beyond Goldwater-Nichols: US Government and Defense Reform for a New Strategic Era, Phase 2 Report* (Washington: CSIS, July 2005); Barry M. Blechman, Thomas R. Pickering, and Newt Gingrich, *Advisory Committee on Transformational Diplomacy: Final Report of the State Department in 2025 Working Group*, 2007, http://www.state.gov/documents/organization/99879.pdf; Project on National Security Reform (PNSR), *Forging a New Shield* (Arlington, VA: Center for the Study of the Presidency, November 2008); and PNSR, *Turning Ideas into Action* (Arlington, VA: Center for the Study of the Presidency, September 2009).

58. Defense Science Board, *2004 Summer Study on Transition to and from Hostilities,* v, 32.

59. PNSR, *Forging a New Shield*, 526.

60. PNSR, *Turning Ideas into Action*, 56; and PNSR, *Forging a New Shield*, 538–39.

61. PNSR, *Turning Ideas into Action*, 57.

62. Ibid.

63. Jeffrey Buchanan, Maxie Y. Davis, and Lee T. Wight, "Death of the Combatant Command? Toward a Joint Interagency Approach," *Joint Force Quarterly* no. 52 (Spring 2009), 95. At the time of their article, BG Jeffrey Buchanan, USA, was deputy commander for operations, Multi-National Division–Center, Iraq; CAPT Maxie Y. Davis, USN, was deputy, information technology and information resource management for deputy chief of naval operations, communication networks; and Col Lee T. Wight, USAF, was commander, 52nd Fighter Wing, Spangdahlem AB, Germany.

64. LCDR Darin M. Liston, USN, *In the Interagency Process, Mere Coordination Is Not Enough: Toward Joint Government* (Newport, RI: Naval War College, 14 February 2005), 13, 15–16.

65. Lt Col Ted A. Uchida, USAF, *Reforming the Interagency Process* (Maxwell AFB, AL: Air Force Fellows, May 2005), 97.

66. Sunil B. Desai, "Solving the Interagency Puzzle," *Policy Review* (February–March 2005).

67. Coffey, *Improving Interagency Integration at the Operation Level*, 40–42.

68. PNSR, *Forging a New Shield*, 243.

69. Lt Col Harold Van Opdorp, USMC, "The Joint Interagency Coordination Group: The Operationalization of DIME," *Small Wars Journal* (July 2005).

70. Ibid.

71. Murdock and Flournoy, *Beyond Goldwater-Nichols*, 48, 51–52.

72. John Hillen, "The Changing Nature of the Political-Military Interface," remarks by Assistant Secretary of State for Political-Military Affairs John Hillen at the Joint Worldwide Planning Conference, Garmisch, Germany, 30 November 2005.

73. US Senate, Committee on Foreign Relations, "Embassies as Command Posts in the Anti-Terror Campaign," 109th Cong., 2nd sess., 15 December 2006, S. Prt. 109-52, 2.

74. Defense Secretary Robert M. Gates, quoted in Gabriel Marcella, "Understanding the Interagency Process: The Challenge of Adaptation," in *Affairs of State*, 39.

75. ADM Michael Mullen, USN, chairman of the Joint Chiefs of Staff, "Admiral Mullen's Speech on Military Strategy, Kansas State University, March 2010," http://www.cfr.org/publication/21590/admiral_mullens_speech_on_military_strategy_kansas_state_university_march_2010.html.

76. MAJ Mark L. Curry, USA, *The Interagency Process in Regional Foreign Policy* (Fort Leavenworth, KS: School of Advanced Military Studies, 5 May 1994), 23–24.

77. Maj Robert S. Pope, USAF, *Interagency Planning and Coordination for Stabilization and Reconstruction Operations* (Maxwell AFB: Air Command and Staff College, April 2004), 8–9; and Johanna McGeary et al., "Looking beyond Saddam," *Time* 161, no. 10 (10 March 2003). See also George Packer, "War after the War," *New Yorker*, 24 November 2003.

78. GAO, "Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing," GAO-09-904SP, September 2009, 1–2.

79. Albert Zaccor, *Security Cooperation and Non-State Threats: A Call for an Integrated Strategy*, Occasional Paper (Washington: Atlantic Council of the United States, August 2005), 24–25.

80. PNSR, *Forging a New Shield*, 95.

81. Derek S. Pugh and David J. Hickson, *Great Writers on Organizations*, 3rd omnibus ed. (Hampshire, UK: Ashgate Publishing, Ltd., 2007), 149. Lyndall F. Urwick (1891–1983) had experience in both industry and the British Army, was director of the International Management Institute in Geneva and subsequently devoted himself to lecturing and writing about management.

82. Michael Donley is currently the secretary of the Air Force. His 30 years of government service have included positions as a professional staff member on the Senate Armed Services Committee, five years on the National Security Council staff, and positions in both the Department of the Air Force and the Office of the Secretary of Defense. While on the NSC staff, Donley coordinated White House policy on the 1986 Goldwater-Nichols Act and both conceived and organized the President's Blue Ribbon Commission on Defense Management. While serving as a senior fellow at the Institute for Defense Analyses, he was a senior consultant to the Commission on Roles and Missions of the Armed Forces and participated in two studies on the organization of the Joint Staff and the office of the CJCS. "Biography, Michael B. Donley," http://www.af.mil/information/bios/bio_print.asp?bioID=11336&page=1.

83. Michael Donley, *Rethinking the Interagency System, Part 2*, Occasional Paper #05-02, (McLean, VA: Hicks & Associates, May 2005), 9.

84. PNSR, *Forging a New Shield*, viii.

85. Louis J. Nigro Jr., "The Department of State and Strategic Integration: How Reinforcing State as an Institution Will Improve America's Engagement with the World in the 21st Century," in *Affairs of State*, 258–59; JFCOM, "Insights & Best Practices," 2; Secretary of State Hillary Rodham Clinton, "President's Proposed Budget Request for fiscal year 2011 for the Department of State and Foreign Operations," testimony before the Senate Appropriations Subcommittee on State, Foreign Operations, and Related Programs, 24 February 2010; and Office of Management and Budget, "The US Department of Defense 2010 Budget," 1, http://www.whitehouse.gov/omb/assets/fy2010_factsheets/fy10_defense8.pdf. Foreign Service officers (FSO) are commissioned officers of the US Foreign Service. They are the State Department's professional diplomats and fill most of the leadership roles at the DoS headquarters in Washington and at US embassies abroad, including about two thirds of ambassador positions (the other third are political appointees). FSOs are selected through a competitive written and oral exam process called the Foreign Service Exam. See Harry W. Kopp and Charles A. Gillespie, *Life and Work in the US Foreign Service* (Washington: Georgetown University Press, 2008).

86. Secretary of Defense Robert M. Gates, quoted in William I. Bacchus, "Regaining Relevance: Five Steps to Strengthen State," *Foreign Service Journal*, (July/August 2009): 14.

87. For example, see LTC Rickey L. Rife, USA, and Rosemary Hansen, FSO, *Defense is from Mars, State is from Venus: Improving Communications and Promoting National Security* (Carlisle Barracks, PA: Army War College, 1 June 1998).

88. Stewart, "Winning Hearts and Minds," 106.

89. Broadcasting Board of Governors Office of Inspector General, *Report of Inspection: The Bureau of African Affairs*, Report no. ISP-I-09-63, August 2009, 13.

90. Based on a rough cost of $100,000 in salary per person.

91. DoD, *Quadrennial Defense Review Report*, February 2006, 79.

92. DoD, *Quadrennial Defense Review Report*, February 2010, 71. The National Security Professional Development (NSPD) program was initiated by Pres. George W. Bush by Executive Order 13434, "National Security Professional Development," 22 May 2007. According to the Congressional Research Service, the NSPD program has accomplished little, and EO 13434 excludes the military, the Foreign Service, and the intelligence community from the program, citing concerns it would detract from these agencies' already established education and training paths. The CRS recommends congressional legislation and oversight to improve the NSPD program. See Catherine Dale, *Building an Interagency Cadre of National Security Professionals: Proposals, Recent Experience, and Issues for Congress*, RL34565 (Washington: CRS, 8 July 2008).

93. PNSR, *Turning Ideas into Action*, 19.

94. "Executive-driven reforms often lack staying power. . . . The executive branch in the 1990s often sought to use existing agencies for new purposes through the exercise of executive fiat rather than seeking broad, bipartisan reforms. The result was the 'bending' of legacy institutions to new missions, often using Presidential directives and executive findings. . . . These executive-driven innovations had their uses . . . but rarely carried over into successive administrations." Murdock and Flournoy, *Beyond Goldwater-Nichols*, 147. See also Maj J. D. York, USMC, *Militarizing the Interagency* (Newport, RI: Naval War College, 14 February 2005), 13.

95. MAJ Thomas M. Lafleur, USA, *Interagency Efficacy at the Operational Level* (Fort Leavenworth, KS: School of Advanced Military Studies, 26 May 2005), 17–22; and Donley, *Rethinking the Interagency System*, 5.

96. Murdock and Flournoy, *Beyond Goldwater-Nichols*, 146.

97. Donley, *Rethinking the Interagency System*, 8.

98. Murdock and Flournoy, *Beyond Goldwater-Nichols*, 34.

99. Nina M. Serafino, *Department of Defense "Section 1207" Security and Stabilization Assistance: A Fact Sheet*, CRS report RS22871 (Washington: CRS, 7 May 2008), 1; and Public Law 111-32, 24 June 2009, 1895.

100. Ben Lieberman, "Crisis! What Crisis? America's Response to the Energy Crisis," in *Mismanaging Mayhem,* 125.

101. US House of Representatives, "Interagency Cooperation Commission Act," 111th Cong., 1st sess., H.R. 2207, 30 April 2009, 1.

Mission Statement

Strategic Studies Quarterly (SSQ) is the senior United States Air Force–sponsored journal fostering intellectual enrichment for national and international security professionals. *SSQ* provides a forum for critically examining, informing, and debating national and international security matters. Contributions to *SSQ* will explore strategic issues of current and continuing interest to the US Air Force, the larger defense community, and our international partners.

Disclaimer

The views and opinions expressed or implied in the *SSQ* are those of the authors and should not be construed as carrying the official sanction of the United States Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Comments

We encourage you to e-mail your comments to us at: **strategicstudiesquarterly@maxwell.af.mil**. We reserve the right to edit your remarks.

Article Submission

The *SSQ* considers scholarly articles between 5,000 and 15,000 words from United States and international authors. Please send your submission in Microsoft Word format via e-mail or regular mail (hard copy and a CD) to:

e-mail: **strategicstudiesquarterly@maxwell.af.mil**

Strategic Studies Quarterly (SSQ)
Managing Editor
155 N. Twining Street, Building 693
Maxwell AFB, AL 36112-6026
Tel (334) 953-1108
Fax (334) 953-1451

Visit *Strategic Studies Quarterly* online at **http://www.au.af.mil/au/ssq/**

Free electronic subscription at **http://www.af.mil/subscribe**

We encourage you to e-mail your comments to us at: strategicstudiesquarterly@maxwell.af.mil.

"Aim High . . . Fly-Fight-Win"

SSQ Strategic Studies Quarterly Summer 2011 AU Press